Microsoft

Protecting Data and Privacy in the Cloud

Contents

Microsoft understands that for our enterprise customers to realize the benefits of cloud computing, they must be willing to entrust their cloud provider with one of their most valuable assets – their data. In this whitepaper, Microsoft will outline its approach and processes to ensure that our customers' data in our enterprise services including Microsoft Azure, Office 365, Dynamics CRM Online, and Microsoft Intune, remains private. After discussing the issues surrounding privacy in the cloud, we will discuss the ways in which we ensure our services protect privacy when building our services, to operating the services in the datacenter, to ensuring our customers make informed choices to protect their data privacy in the cloud.

Cloud Service Categories

- **Software as a Service** (SaaS). The cloud provider hosts a single application, such as Microsoft Dynamics CRM Online, or a suite of programs such as Microsoft's Office 365, which includes a mix of products such as Exchange Online and SharePoint® Online.
- **Platform as a Service** (PaaS). Users create and run their own software applications while relying on the cloud provider for software development tools as well as the underlying infrastructure and operating system. Microsoft Azure is one such cloud platform.
- **Infrastructure as a Service** (IaaS). Users rent computing power—either actual hardware or virtual machines—to deploy and run their own operating systems and software applications. Microsoft Azure also provides this type of service.

Protecting Data and Privacy in the Cloud—An introduction

For organizations throughout the world—whether governments, non-profits, or businesses—cloud computing has become a key part of their ongoing IT strategy. Cloud services give organizations of all sizes access to virtually unlimited data storage while freeing them from the need to purchase, maintain, and update their own networks and computer systems. Microsoft and other cloud providers offer IT infrastructure, platform, and software "as a service," enabling customers to quickly scale up or down as needed and only paying for the computing power and storage they use.

However, as organizations continue to take advantage of the benefits of cloud services, such as increased choice, agility, and flexibility while boosting efficiency and lowering IT cost, they must consider how the introduction of cloud services affects their privacy, security, and compliance posture. Microsoft has worked to make their cloud offerings not only scalable, reliable, and manageable, but also to ensure our customers data is protected and used in a transparent manner.

Customers' have a number of choices of cloud services and cloud infrastructures to purchase, as detailed in the sidebars. Identifying which cloud model is most appropriate depends on the customer needs, their data protection requirements, and the type of processing they require. Indeed, a "one-size-fits-all" approach may not be appropriate for organizations with many different classes of data. Private or hybrid cloud solutions that allow customers to keep selected data on premises can make good sense for those with specialized data protection requirements.

Microsoft offers a full menu of private and hybrid cloud solutions, and we recently published a whitepaper titled "Microsoft Private Cloud: A comparative look at Functionality, Benefits, and Economics."

Security, of course, is an essential component of strong data safeguards in all online computing environments. (See the related paper titled Information Security Management System for Microsoft Cloud Infrastructure.) But security alone is not sufficient. Consumers' and businesses' willingness to use a particular cloud computing product also depends on their ability to trust that the privacy of their information will be protected, and that their data will only be used in a manner consistent with customer expectations.

Cloud Computing Infrastructure

- **Public Cloud.** Customers access cloud services and store documents in large datacenters equipped with hundreds of virtualized servers that house data from multiple organizations.
- **Private Cloud.** A single organization uses a dedicated cloud infrastructure.
- **Community Cloud.** A private cloud is shared by a group of organizations with common missions, interests, or concerns. For example, a cloud provider may offer an instance of their services in a cloud dedicated for only government customers.
- **Hybrid Cloud.** A private cloud is extended to the public cloud to extend an organization's datacenter; or two or more cloud types are linked to enable data and applications to flow between them in a controlled way.

Microsoft has been a leader in creating robust online solutions that protect the privacy of our customers for twenty years. Today, we operate more than 200 cloud and online services that serve hundreds of millions of customers across the globe. Our enterprise cloud services, such as Office 365 and Microsoft Azure, serve millions of end users whose companies entrust their mission-critical data to Microsoft.

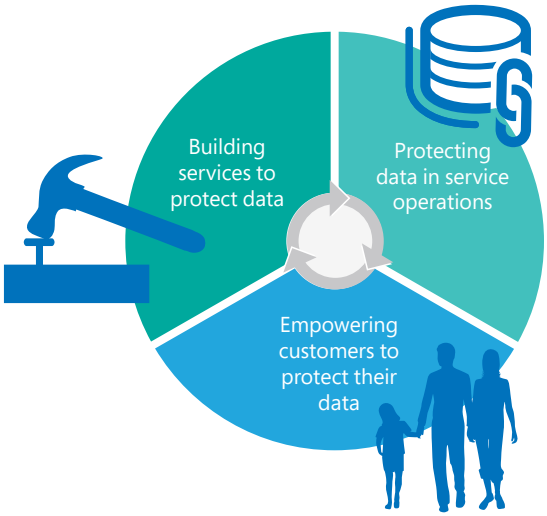
Our experience has enabled us to develop industry-leading business practices, privacy policies, compliance programs, and security measures that we apply across our cloud computing ecosystem. We recognize that cloud services may pose unique security and privacy challenges, and we believe that our time-tested policies and practices provide a solid foundation for addressing customer concerns and enabling greater trust in cloud computing.

Our approach to privacy and data protection in our cloud services is built on a commitment to empower organizations to control the collection, use, and distribution of their information. By providing this functionality and implementing strong operational protection practices, Microsoft can make compliance commitments to our customers in the form of certifications, attestations, and contractual agreements. Microsoft was one of the first organizations to sign European Model Clauses, documenting our commitments to protect the data of our customers who do business in E.U. countries. Commitments to the E.U. Model Clauses, along with standards like the Generally Accepted Privacy Practices (GAPP) and the Fair Information Practice Principles (FIPPs) guided the creation of Microsoft's own privacy principles used to manage customer and partner information.

Together, our privacy principles, data processing agreements and our corporate privacy policy govern the collection and use of all customer and partner information at Microsoft and give our employees a clear framework to help ensure privacy compliance companywide.

We regularly review the privacy policies and codes of conduct that govern our online applications, and we update them periodically if changes are needed to address consumers' evolving needs and expectations.

Our efforts to implement privacy and data protection measures across our cloud service offerings fall into three main areas.



First, we build cloud services from the ground up to protect customer data. Second, we use standards-based techniques and approaches to protect customer data in the datacenter when services are running. Third, we educate customers so that they can make the best decisions possible to protect their data and meet compliance requirements applicable to their business.

The remainder of this paper will delve into the specifics behind each of these approaches.

Building Services to Protect Data

Microsoft encourages all cloud providers to build services that protect not only the integrity of systems and the data itself, but maintain their customers' privacy as well. At Microsoft, we leverage our experience building enterprise software solutions to help identify the privacy and protection requirements our customers need to trust our services.

Key areas in building cloud services to protect customers' data.

- **Making strong commitments** to protect and limit use of customer data.
- **Following "Privacy by Design" principles** to create services from the ground up that take customer privacy into account.
- **Delivering features** that help customers protect and control the flow of their information in cloud services.

Commitments to Protect and Limit Data Use

Microsoft believes that the data that our enterprise customers host in cloud services belongs to them—and should not be used by a cloud provider for purposes other than to provide the customer's service. We put this concept in our enterprise cloud service agreements, and explain this on our Trust Center websites. We define customer data as "all the data, including all text, sound, software or image files that a customer provides, or are provided on the customers' behalf, to Microsoft through use of the Online Services." We do not use customer data for purposes unrelated to providing the service, such as advertising. Additionally, each service has established a set of standards for storing and backing up data, and securely deleting data upon request from the customer.

Privacy by Design

When Microsoft envisions a new product or service, privacy and data protection are considered at each phase of development. This is part of our approach to Privacy by Design, which describes not only how we build products, but also how we operate our services and structure our internal governance practices. This comprehensive approach includes all of the people, processes and technologies that help to maintain and enhance privacy protections for our customers.

Privacy considerations are embedded through the Microsoft Secure Development Lifecycle (SDL). The SDL is a software development process that helps developers build more secure software and address security and privacy compliance requirements while reducing development costs. All of Microsoft's cloud services use the SDL to help ensure that the service and its features are secure and address data protections and privacy requirements.

The SDL is made up of seven phases, including training for developers and program managers in the foundational concepts, building secure software that protects privacy, and responding to security and privacy incidents when they occur.

One of the tools used to drive consistent privacy practices during development is the Microsoft Privacy Standards (MPS), which define standard privacy features and practices. Because security is critical to privacy, this alignment of complementary privacy and security processes helps minimize vulnerabilities in software code, guard against data breaches, and helps to ensure that developers factor privacy considerations into Microsoft products and services from the outset. Microsoft Azure, Office 365, Dynamics CRM Online, and all other business-targeted cloud services use the processes documented in the SDL and the MPS. As part of our commitment to sharing best practices with the technology industry and the privacy community, we have released a public version of our Privacy Guidelines for Developing Software Products and Services.

As part of the development process, privacy reviews are performed to verify that privacy requirements are adequately addressed. For Microsoft cloud services these reviews:

- Verify the presence of privacy-related features that allow customers to control who can access their data and configure the service to meet the customer's regulatory privacy requirements.
- Identify privacy risks.
- Identify required mediation actions so the Microsoft engineering group can implement them.
- Determine, in a final review, whether all requirements were met.

Additionally, as part of our Trustworthy Computing initiative, we employ more than 40 people full-time whose sole focus is protecting privacy. There are over 100 other employees whose job responsibilities include maintaining data privacy. Some of these employees reside in the cloud service product groups to help ensure each service meets corporate privacy requirements. These employees work in tandem with the Trustworthy Computing privacy group, which provides guidance, education, and governance enforcement on privacy issues to employees throughout the company.

Service Features to Protect Privacy

In addition to investments and processes that are in-place to protect customer privacy, Microsoft implements advanced data protection and security features in its services. For example, Office 365 and Dynamics CRM Online both take advantage of Microsoft Azure Active Directory, a comprehensive identity and access management cloud solution. When customers create accounts in either of these services, they are automatically granted an Active Directory cloud account, enabling a seamless single sign-on experience for their users. They can even extend their on-premises directory to Microsoft Azure Active Directory so that users can authenticate with one set of corporate credentials to their cloud-based resources.

By automatically including a Microsoft Azure Active Directory account with an Office 365 or Dynamics CRM Online subscription, Microsoft enables its customers to take advantage of many security and privacy features provided by its directory service. These include:

- Federated identity and access management.
- Rights Management Service

- **Federated identity and access management** when customers subscribe to multiple services. Organizations can use the same Active Directory accounts when they subscribe to Office 365, Dynamics CRM Online, and other Microsoft services, such as Microsoft Intune. Organizations can also leverage Microsoft's support for hybrid clouds by federating identity across services and with their existing on-premises Active Directory service. This gives administrators a single place to manage access to corporate resources both on-premises and in the cloud, thus reducing complexity and improving end-user experience. To learn more about Microsoft's support for hybrid clouds, see the Hybrid Cloud page on the Microsoft Server and Cloud Platform site.

- **Rights Management Service** (RMS). Using RMS, organizations can augment their data protection strategy by protecting information through persistent usage policies that remain with the information, no matter where it is stored. Office 365 includes RMS functionality so that emails, and documents such as those created by Word, Excel and PowerPoint can be RMS protected to help safeguard sensitive information. Users can define who can open, modify, print, forward, or take other actions with the information. Organizations can create custom usage policy templates such as "confidential—read only" that can be applied directly to the information.

In addition to these Active Directory features, Office 365's Exchange Online email service includes a powerful Data Loss Prevention (DLP) service. DLP helps organizations identify, monitor, and protect sensitive information through deep content analysis. DLP is increasingly important for enterprise message systems because business critical email includes sensitive data that needs to be protected. DLP can scan emails for financial information, personally identifiable information (PII) and intellectual property data and take action, such as blocking the data from being sent externally or requiring encryption, should an email be found to contain matching content.

Protecting Data in Service Operations

The best-designed and implemented service cannot protect customer data and privacy if it is deployed to an environment that is not secure. Customers expect that their data will not be exposed to other cloud customers. They also assume that the processes used at the datacenter, and the people who work there, all contribute to keeping their data private and secure.

Doing this takes planning, coordination and a well-trained team. In this section, we will describe the processes and protocols we use to keep customer data private when we run our services. We will also highlight key data privacy standards that govern our services, to ensure customers that the company meets its privacy obligations and commitments, and explain how the services help customers meet their regulators' IT privacy and security requirements. Additionally, we will discuss our commitment to transparency to our customers so that they can demonstrate their compliance to regulators, government agencies, and their own customers.

Microsoft Cloud Service Trust Centers

Dynamics CRM Trust Center
crm.dynamics.com/trust-center

Office 365 Trust Center
trustoffice365.com/

Microsoft Azure Trust Center
azure.microsoft.com/en-us/support/trust-center/

Microsoft Intune Trust Center
microsoft.com/en-us/intune-trust-center/default.aspx

Techniques to Protect Privacy in the Service

There is a set of common techniques that our Microsoft cloud services use to protect data privacy as we operate the service.

The first are data access controls. Data access controls fall into two categories: physical and logical. On the physical side, access to datacenter facilities is guarded by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multi-factor access control, integrated alarm systems, and extensive 24x7 video surveillance from the operations center.

Access to customer data is restricted based on business need. Access is restricted by controls such as role-based access control, two-factor authentication, minimizing standing access to production data, and logging and auditing of activities performed in the production service environment.

Microsoft regularly monitors our production environments for privacy and security-related threats. We use a robust internal program that reports potential privacy risks in our datacenters. When activated, the process brings engineers together with specialists with a background in privacy, forensics, legal, and communications who work as a team to determine the appropriate course of action to ensure that privacy incidents are driven to resolution in a timely manner.

To ensure data privacy between customers who store data in the same cloud service, Microsoft uses data isolation techniques to logically separate cloud tenants and create an environment where customers can only access their own data.

Data geo-location is an important concept for customers operating in regulated industries or in countries with data protection laws. Microsoft understands that some customers must maintain their data in a specific geographic location, such as maintaining data within the EU or APEC. Microsoft's Global Foundation Services (GFS) team maintains a world-wide network of cloud-scale datacenters and verifies each meets strict security requirements.

Each Microsoft cloud service has its own geo-location policies for customer data. The policies are publicly available on each service's Trust Center, and enables customers to know the regions in which their data will be located before they sign up for the service. For more information, visit the Trust Center for the service you are interested in.

This image provides an overview of the regions where Microsoft maintains datacenters for our enterprise cloud service. Many of our services, including Office 365 and Microsoft Azure, offer customers a choice of where to locate their data.

We continuously monitor all systems involved in our services to help identify potential threats by predicting malicious behavior and monitoring for irregular events that may indicate those threats. This monitoring also provides the data for our privacy effectiveness reports that are required by standards organizations.

Data Privacy Standards Compliance

Microsoft Azure, Office 365, Microsoft Intune, and Dynamics CRM Online, not only comply with global data privacy standards, but help enable our customers to comply with those standards as well. Some of these standards include:

HIPAA and HITECH. The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are United States laws that apply to certain healthcare-related entities with access to Protected Health Information, or PHI. We not only offer a platform that enables our customers to comply with these laws, but we offer a Business Associate Agreement (BAA) that documents our obligations for complying with aspects of the law. Office 365, Microsoft
Azure, Microsoft Intune, and Dynamics CRM Online all offer the BAA as part of their service agreements. To learn more, visit the Trust Center for the service that you are interested in.

CSA STAR Registry. Microsoft Azure, Office 365, and Dynamics CRM Online each participate in the Cloud Security Alliance (CSA) STAR Registry program, which allows customers to compare the compliance posture of participating cloud services. To participate, Microsoft summarizes its control activities in accordance with the CSA Cloud Controls Matrix (CCM), which outlines fundamental security principles to guide cloud vendors and to assist prospective customers in assessing the overall security risk of a cloud provider. By submitting our controls activities in accordance with the CCM, we help our customers feel confident in how we protect their privacy and secure their data. Detailed papers that discuss how our services fulfill the security, privacy, compliance, and risk management requirements defined in the CCM are published in the CSA's Security Trust and Assurance Registry (STAR).

For background on the Model Clauses and Microsoft's response to them, read *Why Cloud Customers Can't Ignore Model Clauses, Especially Now*. Also, visit the Trust Center for the Microsoft cloud service you are interested in to see how they comply with these model clauses.

EU Model Clauses. The European Union's 28 data protection authorities, acting through their "Article 29 Working Party," have determined that the contractual privacy protections Microsoft offers to its enterprise cloud customers meet the current existing EU standards for international transfers of data. Microsoft is the first and only cloud provider to receive this type of approval. Europe's privacy regulators have said, in effect, that personal data stored in Microsoft's enterprise cloud is subject to Europe's rigorous privacy standards no matter where that data is located. This recognition applies to Microsoft's enterprise cloud services – in particular, Microsoft Azure, Office 365, Microsoft Dynamics CRM and Microsoft Intune.

ISO 27001. Microsoft's enterprise services, including Office 365, Microsoft Azure, Microsoft Intune, and Dynamics CRM Online are ISO/IEC 27001 certified, and evidence of certification is available through our auditor. Refer to each service's Trust Center for a link to their ISO certification.

SOC1 and SOC2. Microsoft Azure, Office 365, Microsoft Intune and Dynamics CRM Online have each attested to the effective operation of the controls protecting their service in accordance with the AICPA's SSAE16 Service Organization Control (SOC) reporting framework for SOC 1 Type 2 requirements. SOC1 Type 2 attests to the design and operating effectiveness of controls implemented by a service provider. In addition, Microsoft Azure and Microsoft's datacenters have attested to their implementation of controls required for the SOC 2 Type 2 audit, which includes an examination of services for controls related to security, availability, and confidentiality. When this paper was written, Office 365 and Dynamics CRM Online were in progress of completing their SOC2 reports. More information about these reports are available on the Trust Center for each service.

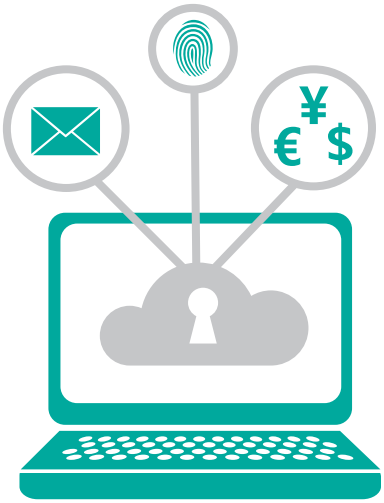
Microsoft will only provide data to lawful requests for specific sets of data.

Transparency

Regarding requests for customer data from law enforcement or other governmental entities, Microsoft is firm in its commitment to protect your data. We will only provide data to lawful requests for specific sets of data. For our enterprise services like Microsoft Azure and Office 365, Microsoft believes that its customers should control their own information whether stored on their premises or in a cloud service. Accordingly, we will not disclose Customer Data to a third party (including law enforcement, other government entity or civil litigant) except as customers direct or required by law. Should a third party contact us with a demand for Customer Data, we will attempt to redirect the third party to request it directly from our customer. If compelled to disclose Customer Data to a third party, we will promptly notify our customer and provide a copy of the demand, unless legally prohibited from doing so. Microsoft also publishes a Law Enforcement Requests Report that provides insight into the scope of requests, as well as information from Microsoft's General Counsel about how the company responds to national security requests.

For more information see the Responding to government legal demands for customer data blog post on the TechNet site.

In addition, the Microsoft Approach to Cloud Transparency paper provides an overview of how we address various risk, governance, and information security frameworks and standards, including the CSA CCM.



Empowering Customers to Protect Their Data

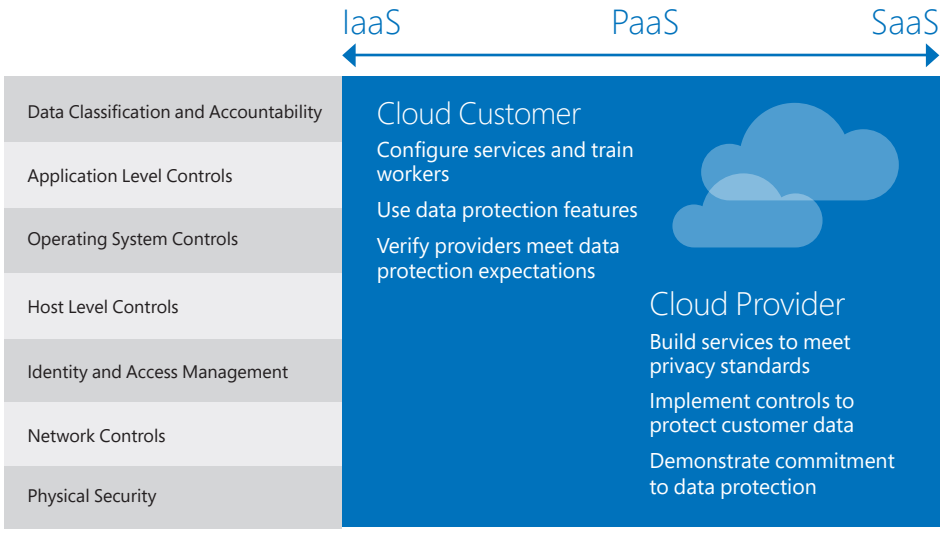
The last of the three areas that Microsoft concentrates on to ensure that customer data remains private is to give its customers and potential customers enough information to make informed decisions about not only how Microsoft protects their data, but also the privacy commitments that the company has made, and the level of responsibility that the customer must take to ensure their data remains secure.

The Data Protection Responsibility Spectrum

Microsoft takes seriously its commitments to protect and maintain the privacy of its customer data—and empowers its customers to implement and use our services in a protected manner. Data protection and privacy is a shared responsibility between the provider and its customers. The provider should be responsible for the platform and accountable for creating a service that can meet the security, privacy, and compliance needs of its customers.

Customers are responsible for configuring and operating their service after it has been provisioned, including managing access credentials and regulatory and legal compliance, protecting applications through the service's configurable controls, data content, and any virtual machines or other data that they use with their account.

The following table breaks down specific cloud provider responsibilities versus the responsibilities of their business customers. The boundaries between these responsibilities is not always clear cut, and can depend on the agreement signed by the customer and other factors. At Microsoft, we work to be as transparent as possible about these roles and responsibilities. We make clear our contractual commitments, publish whitepapers such as this one, and detail service specific considerations on each of our cloud services' Trust Centers.



While providers are responsible for building services and features that facilitate compliance with applicable data protection and privacy regulations and standards, it is up to the customer to configure services and train their workers to use those services in a way that maintains compliance requirements for its industry and location. Also, though it is up to the provider to create strong operational controls to protect customer data in the cloud, it is up to the customer to use those controls in a way that limits unintended data sharing and access. Finally, the provider is responsible for demonstrating its commitment to data protection by obtaining certifications, sharing attestation reports, and signing agreements. However, it is the cloud customer's responsibility to verify that the provider's audit reports, certifications and other evidence meet its organizational data protection expectations.

Microsoft maintains that all customer data remains the property of its customers.

Data Portability

Many of our services enable our customers to download a copy of their data without requiring assistance from us or our partners.

For example, Office 365 supports this through supplying import and export wizards for Exchange Online so that end users can download emails, calendar appointments, contacts, and tasks to their local computers at any time. Additionally, this service provides Windows PowerShell "commandlets", or scriptable commands used to administer Microsoft PowerShell-compatible services, which enables administrators to download end-user metadata as necessary. Finally, when a customer terminates its subscription to Microsoft's enterprise cloud services, Microsoft retains data in a limited function account for at least 90 days to extract its data. Thereafter, data is deleted. This helps ensure that the customer has plenty of time to migrate this data to other services as required by their business. It also ensures that customer data is deleted within in the specified time period so that former customers' data privacy is maintained.

Other Microsoft cloud services have similar policies data portability, data retention, and data deletion policies. To learn more about a specific service's policies, visit the appropriate Trust Center.

Partner Solutions

Microsoft works with an extensive partner network to extend and expand its products and services. This applies to all of its cloud service offerings. To qualify as a partner, an organization must meet specific technical competencies and document that the employees who will work with Microsoft cloud services have passed specific Microsoft certification exams. Then the organization can create new features for and extend existing ones provided by Microsoft's services.

Each service has its own partner programs and certification requirements. To learn more, see the home pages for the service you are interested in.

For data protection and privacy, Microsoft has Identity and Access partners that provide solutions to help customers access and protect information in their cloud solutions. Partners also provide solutions for single sign on (SSO), federated identity, authentication, and for securing data.

By providing guidance and transparency to our customers, we are enabling them to make informed decisions on how to handle their data privacy.

Resources to Empower Customers

Another way that Microsoft empowers its customers to make informed decisions around data protection and privacy requires the company to be as transparent as possible with its policies and communications. To enforce this, the company requires their services to:

- **Maintain an online Trust Center or a privacy statement.** Office 365, Dynamics CRM Online, Microsoft Intune, and Microsoft Azure each have a dedicated Trust Center. Other Microsoft cloud services have a dedicated privacy statement posted online.
- **Document features of the service that impact customers' data privacy.** Microsoft's enterprise cloud services provide documentation describing features that may impact data privacy. For example, Office 365 maintains a features page for small business customers that describe the advanced privacy options for administrators. Office 365 maintains a similar page for administrators of midsize or enterprise-scale businesses, educational and governmental organizations.
- **Provide customers access to law enforcement request reports**. Anyone can view a report summarizing requests that law enforcement agencies around the world have made to Microsoft. This report contains data about the number of requests the corporation receives, documents the number of requests that relate specifically to Microsoft's enterprise cloud services, and details how many requests Microsoft granted and denied. Additionally, last year Microsoft requested that the Attorney General of the United States permit the company to share publicly greater detail about how it handles national security requests for customer information. For more information see the Responding to government legal demands for customer data blog post on the TechNet site. You can also review the law enforcement request report to see where many of these requests have originated, how many we have rejected, and how many we have replied to with the requested data.
- **Post service-specific privacy whitepapers and Cloud Security Alliance (CSA) STAR entries**. Microsoft also requires its services to post privacy whitepapers that outline Microsoft's broad approach to protecting data as well as how privacy considerations are met for each service. Many services provide links to CSA-hosted documentation on their Trust Centers that document how the service complies with CSA STAR requirements.

Conclusion

By building our cloud services with privacy considerations from the outset, and providing compliance mechanisms within our cloud offerings, we are delivering on our commitment to prioritize our customers' data protection needs.

Cloud computing offers organizations and individuals' enhanced choice, flexibility, and cost savings. To realize such benefits, however, cloud customers must have reliable assurances from cloud providers regarding the privacy and security of their data. Regulators and lawmakers around the world have helped fulfill the potential of cloud computing by providing standards and metrics to help both providers and customers define data privacy requirements.

Security and customer data privacy are paramount issues that Microsoft worked on since we began delivering cloud services more than twenty years ago. Since then, our experience has shaped our corporate privacy policies, our product and service development guidelines, and our business practices—all of which we are now adapting
to our newer cloud services.

We are committed to maintaining the highest standards of privacy and security in our online services, and we look forward to continue working with our customers to implement improvements in our data privacy and protection practices and to build on the trust that our customers have placed in our cloud computing services.

Additional Resources

Whitepapers & blog posts

- Information Security Management System for Microsoft Cloud Infrastructure
  http://aka.ms/mgmtcloud
- Privacy Guidelines for Developing Software Products and Services
  http://aka.ms/privdev
- Microsoft Approach to Cloud Transparency
  http://aka.ms/msftcloudtransp
- Microsoft Intune Privacy Practices
  http://aka.ms/msftintuneprivacy
- Responding to government legal demands for customer data
  http://aka.ms/customerdatablog

Websites

- Microsoft Trustworthy Computing
  microsoft.com/en-us/twc/default.aspx
- Cloud Security Alliance Security Trust and Assurance Registry (STAR)
  https://cloudsecurityalliance.org/star/

Microsoft Cloud Service Trust Centers

- Microsoft Dynamics CRM Trust Center
  crm.dynamics.com/trust-center
- Office 365 Trust Center
  trustoffice365.com/
- Microsoft Azure Trust Center
  azure.microsoft.com/en-us/support/trust-center/
- Microsoft Intune Trust Center
  microsoft.com/en-us/intune-trust-center/default.aspx

Trustworthy Computing Next