Privacy in Office 365

Published: August 15, 2016

Introduction

The advances and increased adoption of cloud computing raise important policy considerations, including shared data storage, geographic location, transparency, access, and security. In addition, conflicting legal obligations and competing claims of governmental jurisdiction over data usage continue to limit cloud computing services and their adoption. Divergent rules on privacy, data retention, and other issues cause ambiguity and create significant legal challenges.

Microsoft has been addressing privacy issues associated with cloud computing and online services since the launch of the Microsoft Network in 1994. Microsoft remains committed to protecting the privacy of its customers. We understand that strong privacy protections are essential for building trust in the cloud and helping cloud computing reach its full potential. That's why we built Office 365 with strong data protection in mind with a dedicated team of privacy professionals.

Privacy at Microsoft

As part of our long-term commitment to Trustworthy Computing, Microsoft strives to earn and strengthen trust by building robust privacy and data protections into our products and services. The Trustworthy Computing Group at Microsoft focuses on creating and delivering secure, private, and reliable computing experiences based on sound business practices. The privacy group within Trustworthy Computing manages our privacy governance program, which includes ongoing employee training, identification of emerging privacy issues in the industry, and regular updates to our privacy standards. We work to responsibly manage and protect the data we store, to be transparent about our privacy practices, and to offer meaningful privacy choices. These three tenets—responsibility, transparency, and choice—are the foundation of Microsoft's approach to privacy.

Microsoft privacy principles and privacy standards guide the collection and use of customer and partner information at Microsoft and give our employees a clear framework to help ensure that we manage data responsibly. To put our principles and standards into practice, we have invested heavily to build a comprehensive privacy governance program. Microsoft employs many full-time privacy professionals, with several hundred other employees helping to ensure that privacy policies, procedures, and technologies are applied across our products and services. In addition, Microsoft's global privacy community helps to ensure that the company's privacy policies, procedures, and technologies are applied within our business units. This community includes a three-tiered group of privacy champs, leads, and managers who work with developers, marketers, lawyers, and business executives to review Microsoft products and services and provide guidance on privacy-related issues.

Microsoft Corporate Privacy Policy and Microsoft Privacy Standard

The Microsoft Corporate Privacy Policy comprises six key privacy principles for the protection and appropriate use of customer information, such as information submitted by customers, data obtained from third parties, and data that is automatically collected. Microsoft's six key privacy principles are:

1. **Control** We will put you in control of your privacy with easy-to-use tools and clear choices.
2. **Transparency** We will be transparent about data collection and use so you can make informed decisions. Customer data is kept secure and private. Microsoft only uses customer data to provide online services, including purposes compatible with providing those services. Access to Office 365 data is strictly limited.

3. **Security** We will protect the data you entrust to us through strong security and encryption. We are committed to help protect the data you entrust to us through robust security policy and encryption.
4. **Strong legal protections** We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.
5. **No content-based targeting** We will not use your email, chat, files or other personal content to target ads to you. Microsoft only uses customer data as required to provide services, including purposes compatible with providing those services. Microsoft will not use customer data or derive information from it for the purpose of advertising or similar commercial purposes without permission.
6. **Benefits to you** When we do collect data, we will use it to benefit you and to make your experiences better. Microsoft is responsible for protecting customer data with the same care and precautions it uses to protect its own data. Microsoft only uses customer data as required to provide online services, and to troubleshoot, personalize, and improve online services.

For more information about the implementation of these privacy principles in Office 365, see the Office 365 Online Service Terms. These six principles form the foundation of Microsoft's approach to privacy and will continue to shape the way we build our products and services. In-line with these principles, Microsoft's privacy standards govern the privacy aspects of the development and deployment of Microsoft consumer and enterprise products and services, including Microsoft's cloud services. It informs Microsoft employees and vendors about how to develop products and services with users' privacy in mind so that users are able to better understand and control the collection, storage, retention/destruction, and use of their data.

Privacy Reviews

Like all of Microsoft's products and services, Office 365 undergoes privacy reviews that are designed to identify privacy requirements and help product teams follow Microsoft privacy policies and standards and various national and international industry certification standards (e.g., ISO 27001/27018, SOC/SSAE 16, FedRAMP, etc.). The privacy review process identifies privacy risks and remediation plans. Prior to the release of any product or service, a final privacy review confirms that all implementations based on the review findings have been completed and all requirements are met.

Microsoft's Policy Activities for Privacy

Microsoft works with governments, businesses, technology leaders, and civil society to advise on legislative proposals, help align laws across jurisdictions, develop responsible privacy practices, and strengthen self-regulatory mechanisms that support privacy and data protection in the data age. For example, we have long supported baseline US privacy legislation, coupled with industry self-regulation that facilitates the free flow of information, enhances privacy and trust, and encourages innovation. We also support the concept of accountability. Under an accountability model, privacy goals are established in law, but individual organizations are responsible for determining how best to meet those goals. Further, we have supported efforts to create greater interoperability among global privacy frameworks that better allow differing data protection regimes to work together to support compliance, privacy, and innovation. Together with privacy stakeholders from around the world, we are also thinking about how to evolve the frameworks that have governed aspects of the protection of personal data for the data age.

Privacy in Office 365

Microsoft understands that strong privacy protections are essential for building trust in cloud computing, and implements them in Office 365 as follows:

- **Data use** Microsoft details how it manages and uses customer data, and provides explicit statements that Microsoft uses customer data only for maintaining and securing Office 365 services. Office 365 does not use customer data to create advertisements.
- **Shared data storage** To enable cost savings and efficiencies for data storage, Microsoft stores customer data from multiple customers on the same equipment (known as a multi-tenant architecture). However, the company goes to great lengths to help ensure that multi-tenant deployments of Office 365[1] logically separate the data (and processing) of different accounts and support the privacy and security of the data stored.
- **Data portability** Microsoft enables Office 365 customers to export any or all of their data at any time and for any reason, without any assistance from Microsoft. Even after an Office 365 account expires or is closed, customers by default have limited access for an additional 90 days to export data.
- **Transparency** The Office 365 Trust Center and the Microsoft Trust Center detail the policies and practices that Microsoft uses to protect customer data. The Microsoft Transparency Hub provides customers with direct access to several reports regarding law enforcement and government access to customer data.
- **Access** Microsoft identifies who can access customer data and the circumstances under which they can access it. Microsoft also logs and reports all access to customer data and other critical data. Additionally, Microsoft and its third-party auditors conduct sample audits to help ensure that the customer's data is accessed only for appropriate business purposes.
- **Geographic location of data** For customers interested in knowing where their data is stored, including the assignment of private storage locations, Microsoft tells customers where its major datacenters are located, and how it determines where data is stored at rest. Office 365 administrators can also choose to receive updates to changes in datacenter locations. Microsoft does not control or limit the regions from which a customer it's users may access or move customer data.

Microsoft recognizes that cloud services often raise unique security and privacy questions for business, education, and government customers, so we have adapted our Office 365 policies and governance programs to address customer concerns, facilitate regulatory compliance, and to build greater trust in Office 365 and cloud computing. For example, we contractually commit to specific data handling processes as part of our agreements for Exchange Online, SharePoint Online, Skype for Business, and other cloud services. We also provide customers with flexible management tools that help protect sensitive data and support compliance with government privacy and security guidelines. Such transparent policies and strong tools are essential for our customers as they deal with the privacy and security questions that arise from their use of cloud services.

[1] This link points to a document available on the Microsoft Cloud Service Trust Portal (STP). For information on how to access the STP, see Get started with the Service Trust Portal for Office 365 for business, Azure, and Dynamics CRM Online subscriptions.

Office 365 is built with an emphasis on strong data protection. Reflecting Microsoft's approach to privacy by design, a team of privacy professionals has been dedicated to Office 365 since the beginning of the development cycle and has worked and continues to work in close partnership with engineers, business planners, and marketers. Consequently, privacy has been an integral part of Office 365 from the beginning, not an afterthought. In addition, employees throughout the organization are accountable for managing the service's privacy and security risks. The result is an enterprise cloud service with robust data protections that reflect Microsoft's core privacy tenets of responsibility, transparency, and choice.

Microsoft understands that managing customer information is a responsibility that includes important security and privacy obligations. This is particularly true for cloud-based services such as Office 365. We have a broad network of people and processes that implement our privacy standards and provide privacy guidance and training. If a privacy incident occurs, we have rigorous procedures to address the problem, diagnose the cause, and update customers in a timely manner.

Criteria for determining appropriate levels of privacy and security in the cloud are changing rapidly. What matters most today may be a low priority tomorrow. As a result, when evaluating a cloud provider, organizations would be wise to consider the depth and breadth of the provider's governance model and its ability to quickly adapt to changing privacy priorities.

With Office 365, we have employed a variety of risk management mechanisms to appropriately manage regulatory change, organizational change, personnel change, and technological change. Before any of the services that are part of Office 365 launch to the public, subject-matter experts conduct privacy, security, and business continuity risk assessments on each service and work closely with the service owners to remediate any identified risks. After launch, we use a process of continuous monitoring to ensure that our data protection systems are functioning properly. We test required functionality annually, semi-annually, quarterly, monthly, or at the time of each new release, depending on the level of risk associated with the particular privacy or security control. We also conduct regular risk assessments to refresh the control framework and, if necessary, to reset priorities if new aspects of the service emerge as high-risk. This multi-layered and continuous approach to monitoring the Office 365 data protection environment helps us quickly diagnose and remedy problems that occur and helps our customers respond quickly to shifting regulatory or industry requirements.

Microsoft's Approach to Regulatory Compliance

Just as Microsoft has a responsibility to process our enterprise customers' information in a trustworthy manner, many of our customers have a responsibility to comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data. As a provider of global cloud services, we must run our services with common operational practices and features that span multiple customers and jurisdictions. To fulfill our privacy responsibility to our customers as well as help our diverse customer base fulfill its regulatory obligations, we set the bar high and then build our services to meet that bar using common privacy and security controls. While it is ultimately up to our customers to determine whether our services satisfy their specific regulatory needs, we are committed to providing detailed information about our cloud services to help them in their assessments.

One tool we have developed to facilitate customers' assessments of Office 365 is the Microsoft Trust Center, an online repository of detailed information about Office 365 privacy and security practices. For example, on the Regulatory Compliance page of the Trust Center, we explain how we believe Office 365

helps facilitate compliance with a range of major statutes, from European Union data protection laws to the U.S. Gramm-Leach-Bliley Act, which includes provisions on the protection of consumers' financial information.

Another resource we offer to help customers evaluate Office 365 is detailed information about the well-recognized certifications that the service has attained. On the Security, Audits, and Certifications page of the Trust Center, customers can locate information about the certifications held by both Office 365 and the Microsoft datacenters that host the service. On the Microsoft Cloud Service Trust Portal and within the Service Assurance dashboard, we also enable customers to download third-party audit reports for Office 365, Azure, and more. By making this information readily available, we empower customers to validate that what we say about our security and privacy practices has been affirmed by an accredited third party.

Support for EU-U.S. Privacy Shield

Microsoft supports the recently announced EU-U.S. Privacy Shield, which sets a new high standard for the protection of Europeans' personal data. The Privacy Shield secures Europeans' right to legal redress, strengthens the role of data protection authorities, introduces an independent oversight body, and it clarifies data collection practices by U.S. security agencies. In addition, it introduces new rules for data retention and onward transfer of data. Key Privacy Shield provisions will also be extended to alternative data transfer mechanisms, such as EU Model Clauses. Microsoft has begun the process of implementing the Privacy Shield requirements, which it previously announced it would sign up for in April 2016.

On August 1, 2016, Microsoft signed up for the EU-U.S. Privacy Shield and submitted its Privacy Shield certification to the U.S. Department of Commerce. Going forward, any data which we will transfer from Europe to the United States will be protected by the Privacy Shield's safeguards.[2]

Using Customer Data Only for Providing Services

Responsible cloud providers must have strong internal policies in place that clearly delineate what the provider and its partners can and cannot do with customer information. In Office 365, we use our customers' data only for what they pay us for—to maintain and provide Office 365 services. As part of providing a quality service, we will troubleshoot in order to prevent, identify, or repair problems and to improve features that protect our customers. Microsoft does not build advertising products out of our customers' data. We also don't scan our customers' email or documents for the purpose of building analytics, data mining, advertising, or improving the service without our customers' permission.

Government Access to Customer Data

Microsoft does not provide any government with direct and unfettered access to its customers' data, and Microsoft does not provide any government with its encryption keys or the ability to break its encryption. If a government entity approaches Microsoft directly with a request related to a Microsoft Online Services customer, Microsoft will first try to redirect the entity to the customer to respond. If Microsoft is required to respond to the demand, Microsoft will promptly notify the customer and provide a copy of the demand (unless legally prohibited).

Microsoft publishes its law enforcement requests report to identify the number and types of requests it receives and its compliance with those requests. Microsoft recently received permission from the U.S.

[2] See http://blogs.microsoft.com/on-the-issues/2016/08/01/microsoft-signs-privacy-shield/ for the official announcement.

government to publish information about Foreign Intelligence Surveillance Act orders and National Security Letters.

Trust with Transparency

Although many organizations cite privacy and security concerns as major obstacles to their adoption of cloud services, information on the privacy and security practices of many cloud providers is either difficult to find or indecipherable to all but the most astute IT professionals. To help our customers find answers to their privacy and security questions about Office 365, we strive to be as transparent as possible about our data protection policies and procedures.

The centerpiece of our transparency efforts is the Microsoft Trust Center, which includes several service Trust Centers:

- Office 365
- Microsoft Azure
- Microsoft Commercial Support
- Microsoft Dynamics AX
- Microsoft Dynamics CRM Online
- Microsoft Intune
- Microsoft National Clouds
- Power BI

The Microsoft Trust Center is designed to provide answers to questions that customers have about our cloud services, such as who can access their data, where their data is stored, and how they can verify that Microsoft is doing what it says. Our compliance is independently audited, and we're transparent on many levels—from how we handle legal demands for your customer data to the security of our code. We offer detailed trust information on each of our cloud services. For example, on the Office 365 Trust Center, we describe our approach to security, privacy, compliance, and transparency. We state clearly that customers own their data and that we are the custodian or processor of your data. And that because it is your data, if you ever choose to leave the service, you can take your data with you.

Regulatory Compliance in Office 365

To help organizations comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, Microsoft offers the most comprehensive set of certifications and attestations of any cloud service provider. To demonstrate that these controls deliver compliance you can rely on, Microsoft enterprise cloud services are independently validated through certifications and attestations, as well as third-party audits. In-scope services within the Microsoft Cloud meet key international and industry-specific compliance standards, as well as regional and country-specific standards and contractual commitments. In addition, rigorous third-party audits validate the adherence of our cloud services to the strict requirements these standards mandate.

Customers can view by service, location, and industry, all of the global standards to which Office 365 and other Microsoft cloud services conform on the Compliance page of the Microsoft Trust Center.

Microsoft Privacy Resources

Listed below is a sampling of the privacy resources from Microsoft that are available to customers and prospective customers.

- Microsoft Privacy Practices
- Privacy Guidelines for Developing Software Products and Services
- Microsoft Trustworthy Computing
- Privacy Models
- Microsoft Online Services Privacy Statement
- Cloud Privacy at Microsoft
- Microsoft Transparency Hub - Law Enforcement Requests
- Brad Smith blog post - Responding to government legal demands for customer data
- Brad Smith blog post - Our search warrant case: An important decision for people everywhere
- John Frank blog post - EU-U.S. Privacy Shield: Progress for privacy rights
- EU Policy blogs from Microsoft on Privacy

Microsoft has also created a guide called Building Global Trust Online, 4th Edition: Microsoft Perspectives for Policymakers, which was compiled from extensive work and ongoing research by Microsoft teams, as well as consultation with external subject-matter experts to provide ongoing education about policy topics related to privacy, security, safety, and accessibility.

Summary

Since Microsoft recognizes that privacy and security are major concerns for cloud customers, we developed Office 365 from the ground up with strong data protection in mind. Microsoft's privacy principles and privacy standards guide the collection and use of customer and partner information at Microsoft and give our employees a clear framework to help ensure that we manage data responsibly. The Microsoft Corporate Privacy Policy comprises six key privacy principles for the protection and appropriate use of customer information, such as information submitted by customers, data obtained from third parties, and data that is automatically collected.

Microsoft recognizes that cloud services often raise unique security and privacy questions for business, education, and government customers, so we have adapted our Office 365 policies and governance programs to address customer concerns, facilitate regulatory compliance, and to build greater trust in Office 365 and cloud computing. Reflecting Microsoft's approach to privacy by design, a team of privacy professionals was dedicated to the product early in the development cycle and worked in close partnership with engineers, business planners, and marketers. Consequently, privacy has been an integral part of Office 365 from the beginning, not an afterthought. In addition, employees distributed throughout the organization are accountable for managing the service's privacy and security risks. The result is an enterprise cloud service with robust data protections that reflect Microsoft's core privacy tenets of responsibility, transparency, and choice.