Windows Azure

Windows Azure Privacy Overview

February, 2014

Microsoft

Table of Contents

Introduction

Microsoft recognizes that cloud services are raising unique privacy challenges for organizations. To enable organizations to realize the benefits of the cloud, Microsoft implements strong privacy protections in Windows Azure services and makes commitments to safeguard the privacy of customer data. In addition, Microsoft strives to be transparent so customers have visibility into where their data resides and who has access to it.

In the following pages, we will discuss Microsoft's approach to privacy in the cloud as well as the specific policies, operational practices, and technologies that are in place to help ensure the privacy of your data in Windows Azure.

Microsoft Approach to Privacy in the Cloud

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 Windows 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. Driven by a commitment to empower organizations to control the collection, use, and distribution of their data, our time-tested approach to privacy provides a solid foundation for addressing customer privacy requirements and enabling greater trust in cloud computing.

Your Data in Windows Azure

With Windows Azure, customers own their data. 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 Services.” For example, this includes data that you upload for storage or processing and applications that you run in Windows Azure. Refer to the Windows Azure Trust Center for a detailed understanding of how Microsoft classified data in Windows Azure.

Customers can retrieve their Customer Data at any at any time and for any reason, typically without assistance from Microsoft. When a customer chooses to delete data or leave the service, Microsoft removes the Customer Data from all systems under its control. Upon systems end-of-life, Microsoft operational personnel follow rigorous data-handling procedures and hardware disposal processes.

Location of Customer Data

For many customers, knowing and controlling the location of their data can be an important element of compliance and governance. With Windows Azure, customers can specify the geographic area(s), which we call "geos" and "regions", of the Microsoft datacenters in which their Customer Data will be stored. Available geos and regions are shown in the following table.

Geo	Region
Asia Pacific	Asia Pacific East (Hong Kong) Asia Pacific Southeast (Singapore)
Europe	Europe North (Ireland) Europe West (Netherlands)
United States	US North Central (Illinois) US South Central (Texas) US East (Virginia) US West (California)
Japan	Japan East (Saitama Prefecture) Japan West (Osaka Prefecture)

See the Windows Azure Trust Center for the most up-to-date list of geos and regions and the Windows Azure Regions page for information on our global network of datacenters.

Microsoft may transfer Customer Data within a geo (such as, from Europe North to Europe West) for data redundancy or other purposes. For example, Windows Azure replicates Blob and Table data between two regions within the same geo for enhanced data durability in case of a major datacenter disaster.

Microsoft will not transfer Customer Data outside the geo(s) a customer specifies (for example, from Europe to U.S. or from U.S. to Asia) except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where the customer configures the account to enable such transfer of Customer Data through the use of specific features and services as outlined in the Windows Azure Trust Center.

Microsoft does not control or limit the geos from which customers or their end users may access Customer Data.

Data Access and Use

Access to your data by Microsoft personnel is restricted. Customer Data is only accessed when necessary to support your use of Windows Azure. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of Windows Azure and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). When granted, access is carefully

controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed.

Windows Azure does not share Customer Data with its advertiser-supported services. We also do not mine Customer Data for advertising.

The operational processes and controls which govern access and use of Customer Data in Windows Azure are rigorously maintained and regularly verified by accredited audit firms.

Contractual Commitments

Microsoft makes strong contractual commitments to safeguard Customer Data and provide privacy protections. This includes provisions for customers in geographies or industries with additional controls around personal data.

E.U. Data Protection Directive

European law prohibits companies from transferring personal data from the EU except under specific conditions. One way to transfer such data is to procure cloud services from companies that abide by the U.S.-EU Safe Harbor and Swiss-U.S. Safe Harbor frameworks.

To accommodate the data privacy demands of European entities, Microsoft is Safe Harbor certified under the U.S. Department of Commerce. The Safe Harbor certification allows for the legal transfer of E.U. personal data outside of the E.U. to Microsoft for processing. This addresses the limited instances when data is transferred outside of the customer-specified geographic region. Microsoft also offers additional contractual commitments to its enterprise customers:

- A Data Processing Agreement that details our compliance with the E.U. Data Protection Directive and related security requirements for Windows Azure core features within ISO/IEC 27001:2005 scope
- E.U. Model Contractual Clauses that provide additional contractual guarantees around transfers of personal data for Windows Azure core features within ISO/IEC 27001:2005 scope

HIPAA Business Associate Agreement (BAA)

Windows Azure also complies with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. These are United States laws that apply to healthcare entities with access to patient information (called Protected Health Information, or PHI). In many circumstances, for a covered healthcare company to use a cloud service like Windows Azure, the service provider must sign a written agreement to adhere to certain security and privacy provisions set forth in HIPAA and the

HITECH Act. To help customers comply with HIPAA and the HITECH Act, Microsoft offers a Business Associate Agreement (BAA) to enterprise customers as a contract addendum.

Prior to signing the BAA, customers should read the Windows Azure HIPAA Implementation Guidance to understand the relevant capabilities of Windows Azure. The document covers some of the best practices for building HIPAA compliant applications, and details Windows Azure provisions for handling security breaches.

Subcontractors

Microsoft may hire other companies to provide limited services on its behalf, such as providing customer support. Microsoft will only disclose Customer Data to subcontractors so that they can deliver the services we have retained them to provide. Subcontractors are prohibited from using Customer Data for any other purpose, and they are required to maintain the confidentiality of our customers' information.

We require subcontractors to join Microsoft's Supplier Security & Privacy Assurance Program, to meet our privacy requirements by contract, and to undergo regular privacy training. We contractually obligate subcontractors that work in facilities or on equipment controlled by Microsoft to follow our privacy standards. All other subcontractors are contractually obligated to follow privacy standards equivalent to our own. Download the list of subcontractors to see which companies are authorized to process Customer Data in Windows Azure.

Law Enforcement Requests

Microsoft believes that our customers should control their own data 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 entities or civil litigants) except as our customers direct us or as 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 customers. As part of that, we may provide customers' basic contact information to the third party. We require a court order or warrant before we will consider disclosing content to law enforcement. If compelled to disclose Customer Data to a third party, we will promptly notify the customer and provide a copy of the demand to them, unless legally prohibited from doing so.

Microsoft also publishes a Law Enforcement Requests Report that provides insight into the scope and number of requests. To learn more about how Microsoft responds to requests for Customer Data, read the Responding to government legal demands for Customer Data blog post from Microsoft's General Counsel.

Built In Data Protection

Microsoft designed and implemented the Windows Azure platform to enable our customers to protect their data and its privacy. Windows Azure provides the infrastructure our customers can use to: help

- Control access to their data and applications
- Protect data in transit and at rest
- Securely connect to Windows Azure

Identity and Access

Microsoft offers comprehensive identity and access management solutions for customers to use across Windows Azure and other Microsoft cloud services. Specifically, Windows Azure includes the following features to enable customers to control access to their data and applications:

- **Enterprise cloud directory.** Organizations can sync on-premises identities to Windows Azure Active Directory and enable single sign-on to simplify user access to their cloud applications.
- **Access Monitoring.** Security reports monitor inconsistent access patterns and help to mitigate potential threats.
- **Strong authentication.** Windows Azure Multi-Factor Authentication helps prevent unauthorized access by providing an authentication mechanism in addition to a password.
- **Role-based access control.** Our customers can implement authorization schemes that controls users' access to resources based on their role assignment, their role authorization, and their permission authorization.

Data Encryption and Isolation

Windows Azure safeguards Customer Data using three specific methods: encryption, segregation, and destruction.

- **Data in transit.** For data in transit, Windows Azure uses industry standard transport protocols such as SSL and TLS between user devices and Microsoft datacenters, and within datacenters themselves. IPsec can also be used to create a VPN connection with a Windows Azure Virtual Network (VNET). Customers can enable encryption for traffic between their own Virtual Machines and end users.
- **Data at rest.** Customers are responsible for ensuring that data stored in Windows Azure is encrypted in accordance with their standards. Windows offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Options include.NET cryptographic services, Windows Server public key infrastructure (PKI) components, Microsoft StorSimple cloud-integrated storage,

Active Directory Rights Management Services (AD RMS), and BitLocker for data import/export scenarios.

- **Data isolation.** Windows Azure is a multi-tenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware. Windows Azure Storage uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.
- **Data destruction.** When customers delete data or leave Windows Azure, Microsoft follows strict rigorous standards that call for overwriting storage resources before reuse, as well as physically disposing of decommissioned hardware.

Network Security

Windows Azure networking provides the infrastructure necessary to securely connect VMs to one another as well as to make connections between on-premises datacenters and Windows Azure VMs. Windows Azure blocks unauthorized traffic to and within Microsoft datacenters using a variety of technologies such as firewalls, NATs, partitioned Local Area Networks and physical separation of back-end servers from public-facing interfaces.

- **Isolating Customer Data and networks.** Fundamental to any shared cloud architecture is the isolation provided for each customer. In Windows Azure, a customer subscription can include multiple deployments, and each deployment can contain multiple VMs. Windows Azure isolates deployments and virtual networks from one another. Individual VMs do not receive inbound Internet traffic except through customer-defined endpoints.
- **Encrypting communications.** Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Windows Azure regions, and from Windows Azure to on-premises datacenters. All of these protocols are designed to provide a high default level of network security while giving customers the flexibility and choice to configure Windows Azure to meet business needs. Administrator access to virtual machines through remote desktop sessions, remote Windows PowerShell, and the Windows Azure Management Portal is always encrypted.
- **Using Express Route.** Customers can use an optional Express Route private fiber link into Windows Azure datacenters to keep their traffic off the Internet.

Conclusion and Additional Resources

Microsoft has a longstanding commitment to privacy, which is an integral part of how we build, deploy, and manage Windows Azure. We work to be transparent in our privacy practices, to offer customers meaningful privacy choices, and to manage responsibly the data we store.

We publish detailed information about Windows Azure privacy, security, and compliance in our Trust Center and provide access to audit reports and compliance packages to assist customers in understanding the policies, operational processes, and technologies in place to help safeguard the privacy of their data.

Additionally, customers can read more general information about Microsoft's work to protect Customer Data across all of our cloud services on the Microsoft Cloud Privacy Web Site and in the Privacy in the Cloud white paper.

Additional Resources

- Windows Azure Privacy Statement
- Microsoft Trustworthy Computing Privacy Web Site
- Law Enforcement Request Report
- Data Classification for Cloud Readiness
- CISO Perspectives on Data Classification