

# **Privacy and Microsoft Online Services**

White Paper

March 2009

---

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveX, Outlook, SharePoint, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

# Contents

Introduction: Privacy .....	1
Microsoft Online Services Privacy Strategy .....	1
Implementing Privacy In Our Services .....	1
International Data Transfer .....	5
Vendors, Partners, and other Third Parties.....	5
Conclusion and Further Information .....	6

## Introduction: Privacy

Effective data governance can significantly reduce data breaches—the accidental exposure or outright theft of personal information—and other data security risks, while also lowering costs and increasing organizational efficiency and competitiveness. Data governance is the application of policies and processes designed to extract the maximum value of data held within an organization while also managing risks, enhancing privacy protection, and meeting compliance requirements.

This paper provides an overview of the Microsoft's approach to data privacy and the steps Microsoft Online Services take to help protect customer privacy through a combination of sound privacy principles, technology, business process innovation and investments, and transparency.

## Microsoft Online Services Privacy Strategy

Microsoft Online business and organizational customers can use the functionality of Microsoft Online Services to manage and control their own data.

In order to help create a trustworthy experience for our customers, Microsoft Online Services follows a three-pronged strategy:

1. We develop our software, services, and processes with privacy in mind. We are vigilant in following developments in global privacy laws. Our privacy practices are derived from privacy principles developed around the world. We closely align our privacy practices with applicable laws and strive to apply our practices globally across all services offered.
2. We employ technical and organizational security measures in handling customer data.
3. We are open and transparent about our information handling practices, including the thorough disclosures made in the Microsoft Online Services Privacy Statement.

The underpinning of Microsoft Online Services' privacy practices is that services are operated by Microsoft on behalf of its business customers. Personal data Microsoft collects or handles through Microsoft business services is processed for the customer, not for individuals who may be using the service (for example, employees of the customer). Personal information residing in Microsoft Online Services is only collected, processed, and transferred with the consent of the customer (e.g., to provide the services) or as required under applicable law.\*

## Implementing Privacy in our Services

---

\* Microsoft's customers are responsible for their own compliance with applicable policies, practices, and regulations and for using Microsoft Online Services appropriately (e.g., interpreting relevant privacy laws and regulations; notifying and obtaining consent, as appropriate, from employees and other users about data collection, processing and transfer; and for defining the appropriate level of protection for different classes of personal information).

This section of the Privacy and Online Services White Paper describes the primary privacy features applied across Microsoft Online Services.<sup>†</sup>

### **Privacy Engineered From the Start**

The Microsoft Online platform and services benefit from privacy policies and procedures that Microsoft has built into software development, testing, operations, and maintenance practices. These practices are based squarely on core principles that have come to characterize Microsoft's approach to software development and overall business practices.

The principles are largely embodied in the Trustworthy Computing Initiative. This Initiative was put in place in 2002, when Bill Gates set out the basis that would characterize the effort of "building trust into every one of our products and services." The overall goal of the Initiative is to help deliver a secure, private, and reliable computing experience for everyone.

The Microsoft Security Development Lifecycle (SDL), Microsoft's industry-leading software security development process, is a primary vehicle used to drive Trustworthy Computing principles into Microsoft products and services. Microsoft Online Services follows the SDL for software and service development, deployment and maintenance. The SDL introduces security and privacy early and throughout the development process.

### **Privacy Guidelines for Developing Software Products and Services**

Additionally, Microsoft Online software is built according to the [Privacy Guidelines for Developing Software Products and Services](#). These guidelines provide specific requirements and expectations for developers on creating notification and consent experiences, providing data security, and facilitating controlled user access when developing software products and Web sites. These guidelines reflect the following core privacy principles: notice, choice, access, security, and data integrity.

#### **Notice**

To give users appropriate notice, Microsoft places the [Microsoft Online Services Privacy Statement](#) at appropriate locations on the service. This privacy statement explains Microsoft Online's data handling practices and customer contact policies.

The [Microsoft Online Services Privacy Statement](#) also describes how individual end users may ask questions about Microsoft's data handling practices. When a privacy-related inquiry or complaint is received from a customer's user or employee, Microsoft promptly notifies the customer of the issue and provides the necessary support for response and resolution.

#### **Choice**

Microsoft relies on customers to obtain end users' consent to the collection and processing of data by Microsoft. To assist customers in getting the right consent, the Microsoft Online Services Privacy

---

<sup>†</sup> Microsoft Online Services Dedicated customers can achieve substantially similar features and functionality to those described in this White Paper. For more information about the Microsoft Online Services Dedicated offering,, please contact a Microsoft sales or account manager.

Statement describes how Microsoft uses data. Two areas of Microsoft's data processing practices are highlighted below: marketing and advertising, and testing.

#### Marketing and Advertising:

Microsoft may market to customers who register with and purchase Microsoft Online Services. These customers may choose to opt out of receiving promotional communications from Microsoft Online Services at any time. However, Microsoft does not display third party online advertising to customers' individual end users, or use for marketing or advertising purposes any end user personal information collected in the course of providing Microsoft Online Services, except with the consent of the customer.

Microsoft does not use personal data received as part of utilizing Microsoft Online Services for marketing or advertising purposes. However, if end users *voluntarily* use their Microsoft Online Services credentials to register for or use Microsoft consumer services, such as Windows Live, or otherwise consents, Microsoft may use data collected through such services for the purposes of targeting advertisements, consistent with the consumer services' terms of use and privacy statements.

#### Testing:

Microsoft Online does not use customer personal information for testing except to provide or improve Microsoft's services, or with the explicit consent of the customer. To improve the services, Microsoft may aggregate and anonymize data for planning purposes. Microsoft may also compile a sample set of data from across the services to run through servers before planned updates. (In such cases, all of the safeguards and controls applied in the production systems will be employed in the test environment.) This helps to identify problems early; reduce interruptions to the services; and lower the number of support incidents. Additionally, if we identify spam or malware originating from your account, we may isolate and use this information to improve the security of our network for all users.

#### **Access, Security, Data Integrity and Enforcement**

Microsoft uses a variety of technical and organizational security measures to help protect customer data. These measures include access controls, encryption in transfer (and, in some cases, encryption at rest), physical security, disaster recovery, and auditing. Implementing a security program that considers data protection holistically is essential to helping protect critical business data from compromise and loss. As described in detail on the [MS Online Services Security Overview](#), the safeguards highlighted in the table below form part of Microsoft's overall data protection program.

## A Framework for Managing and Protecting Personal Information

Element	Description
Infrastructure	Safeguards that help protect against malware, intrusions and unauthorized access to personal information and protect systems from evolving threats
Identity and Access Control	Systems that help protect personal information from unauthorized access or use and provide management controls for identity access and provisioning
Information Protection	Helping to protect sensitive personal information in structured databases and unstructured documents, messages and records by means such as encryption with the intent that only authorized parties can view or change it throughout its life cycle
Auditing and Reporting	Monitoring to verify the integrity of systems and data in compliance with business policies

Additionally, in order to help customers maintain control over their own data, Microsoft Online Services are designed to provide a customer's administrators or representatives extensive controls over the customer's environment—including their user's mailboxes and Web sites—to be able to address and enforce the customer's own privacy and security policies. Microsoft also may provide records detailing each administrator's access to user mailboxes in order to support audit needs, and for purposes of monitoring adherence to the customer's policies. These records may also detail access by customer partners and Microsoft's support personnel to user's mailboxes, except when prohibited by law.

In the event Microsoft discovers a security breach of personal information on the Microsoft Online Services that requires notice under applicable law, Microsoft does cooperate with the customer and assist it in fulfilling legal obligations arising out of the incident, to the extent it does not conflict with Microsoft's own legal obligations.

For more information about specific privacy features of Microsoft Online Services, please see the [Microsoft Online Services Privacy Statement](#).

## **International Data Transfer**

Microsoft Online Services goal is to provide business features and functionalities to customers broadly, regardless of location. However, as customers set-up and authorize the accounts of end users on the service, the pull-down menu only displays locales in which Microsoft offers Microsoft Online Services in such a way that data transfer is possible, providing the customer follows applicable law.

Information that is collected by or sent to Microsoft may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities.

Microsoft is Safe Harbor certified with the U.S. Department of Commerce and abides by the Safe Harbor framework regarding the collection, use, and retention of data from the European Union. This allows for the export of personal data to Microsoft from the European Union, as well as countries that accept the Safe Harbor certification for trans-border transfers.

## **Vendors, Partners and Other Third Parties**

### **Vendors**

In order to support the delivery of Microsoft Online Services, Microsoft occasionally provides information to other companies that offer services on Microsoft's behalf. These companies are required to maintain the confidentiality of personal information and are prohibited from using it for any other purpose. Microsoft's Vendor Privacy Assurance Program applies to the use of personal information by Microsoft vendors, which requires them to meet Microsoft's standards for privacy, and enforces this both contractually and through certification and vendor audits.

### **Partners**

If customers procure through Microsoft features or support services provided by Microsoft partners, Microsoft shares personal information with those partners. Microsoft is not responsible for the privacy and information handling practices of such partners. However, Microsoft provides notice when a customer signs up through Microsoft Online Services for a Microsoft partner service that Microsoft transfers personal information to the partner. Additionally, a customer may opt-out of future sharing of information with a partner at any time.

### **Other Third Parties**

As described in the terms governing customer use of Microsoft Online Services, Microsoft may access or disclose personal information, including the content of customer communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or Microsoft customers, including the enforcement of Microsoft agreements or policies governing use of the services; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers or the public.

## Conclusion

Microsoft understands that customers have high expectations about how their data is collected, used, and stored. With these concerns in mind, Microsoft has created and implemented policies and processes for designing, developing, testing, and operating to help ensure that:

- Privacy is engineered into products and services as critical components of the product and service life cycle.
- Privacy-aware technology is implemented throughout Microsoft Online's internal processes.
- Our global privacy practices are properly executed throughout Microsoft Online

## Further Information

[Microsoft Online Services Privacy Statement](#)

[Microsoft's Trustworthy Computing Initiative Privacy Overview](#)

[Privacy Guidelines for Developing Software Products and Services](#)

<http://www.microsoft.com/mscorp/twc/security/overview.mspx>