

# Trustworthy Computing



## Managing and Protecting Personal Information

*A Microsoft Perspective on Data Governance  
for Privacy and Compliance*

November 2008

The information contained in this document represents the current view of Microsoft Corp. 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 OR IMPLIED, 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.

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.

© 2008 Microsoft Corp. All rights reserved.

Microsoft is a registered trademark of Microsoft Corp. in the United States and other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

# Contents

- Executive Summary ..... 1
- The Landscape ..... 2
- A Complicated Mix of Laws..... 3
- What Is Data Governance?..... 5
- The Information Life Cycle ..... 6
  - Data Governance and the Information Life Cycle ..... 8
- A Technology Framework for Data Governance ..... 9
  - Secure Infrastructure..... 9
  - Identity and Access Control..... 10
  - Information Protection..... 11
  - Auditing and Reporting ..... 12
- Principle-Based Application of the Technology Framework ..... 12
- The Role of Government in Data Governance ..... 13
- Conclusion ..... 13

## Executive Summary

As the collection and use of personal information in digital form become increasingly prevalent, widely publicized security and data breaches and growing public concerns about identity theft threaten to curtail the growth of online commerce and services. Governments and organizations that fall short in effectively managing and protecting users' personal information face considerable risks—including damage to their reputation, penalties and sanctions, lost market share and needless expense.

Fortunately, research shows that effective "data governance" can significantly reduce data breaches—the accidental exposure or outright theft of personal information—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 ensuring that compliance requirements are met. A holistic approach to data governance begins with an understanding of the information life cycle—the collection, updating, processing and eventual deletion of personal information—and the adoption of a technology framework that enables governments and organizations to set controls which safeguard individuals' privacy.

To encourage businesses and organizations to take a holistic approach to data governance, governments can set an example by embracing these principles and practices themselves. Governments can also help protect citizens by working with industry to adopt effective standards and policies on data retention, reduce the risk to users' privacy that comes with unneeded and long-term storage of personal information, and take appropriate action when breaches do occur. Comprehensive data breach notification legislation is another important step that can help keep citizens informed of serious risks to their online identity and financial information as well as strengthen consumer confidence in online commerce and services.

## The Landscape

In the past three decades, information and communications technology (ICT) has helped to transform the global economy and enable private enterprises and governments to achieve unprecedented results. Greater productivity, more efficient internal processes and new ways of collaborating within organizations and with partners and customers are helping companies of all sizes to compete more effectively in fast-paced global markets. Governments are also taking advantage of these advances to operate more efficiently and deliver services more effectively to citizens.

The massive and rapid flow of personal information over the Internet has played a key role in this transformation by supporting intelligent data analysis, expanded sales and service channels, and more innovative approaches to addressing organizational challenges. Yet, as organizations handle growing volumes of personal data and use it in an increasing variety of ways, they also face more compliance requirements and a greater responsibility to adequately protect the privacy and integrity of this data.

Many consumers, business leaders, government policymakers and privacy advocates are calling for more effective policies, processes and technologies to protect and manage the personal information entrusted to organizations. These organizations must balance the desire to optimize the flow, utility and value of this information with the responsibility to safeguard it from loss, theft and misuse.

Meanwhile, protecting users' privacy and keeping their information secure have become more difficult. Widely publicized security and data breaches and rising consumer anxiety about identity theft and the privacy of personal information are eroding public trust in the Internet and threatening to dampen online services and commerce. For example:

- According to DataLossDB, a nonprofit organization that tracks data breach incidents, at least 162 million records containing personal data were compromised worldwide in 2007, compared to 49 million records in the previous year.<sup>1</sup>
- In November 2007, the UK tax agency Her Majesty's Revenue and Customs disclosed that it had lost computer disks containing the records of 25 million UK residents—about 40 percent of the population—including confidential information such as names, addresses, dates of birth and bank account data.
- In January 2007, U.S. retailer TJX Companies disclosed the largest breach on record, in which an identity theft ring stole data on 45.6 million payment cards, exposing 100 financial institutions to losses from fraud.
- More than 90 percent of Chinese worry that their private details are too easily divulged and misused, and more than 74 percent want tougher laws on privacy and related infringements, according to a national survey conducted by *China Youth Daily* in December 2007.

---

<sup>1</sup> Source: DataLossDB, <http://datalossdb.org/>.

- A 2008 InformationWeek survey of 1,100 IT and business professionals found that 66 percent felt they were as vulnerable, or more vulnerable, to breaches and malicious attacks as they were in the previous year.<sup>2</sup>

### Privacy and Data Protection at Microsoft

Microsoft's commitment starts with the people, policies and processes that make privacy and data protection an integral part of the company's business practices and corporate environment.

**Privacy staffing:** Microsoft implements its privacy goals internally through three levels of staffing. The Microsoft Corporate Privacy Group manages the development and implementation of programs that enhance the privacy of Microsoft products, services, processes and systems. Many business units have full-time privacy staff, and several hundred other employees are responsible for helping to ensure that privacy policies, procedures and technologies are applied within the product groups and subsidiaries in which they work.

**Privacy policy:** Microsoft's approach to privacy and data protection is based on a belief that individuals should be empowered to control the collection, use and distribution of their personal information. Microsoft's corporate privacy policy incorporates 10 principles that apply to all customer and partner information, including accountability, notice, collection, choice and consent, use and retention, disclosure, quality, access, security and monitoring, and enforcement. This policy gives business units and employees a clear and simple framework to help ensure privacy compliance.

**Privacy guidelines:** The Microsoft Privacy Guidelines for Development set a framework to help ensure that customer privacy and data protections are systematically incorporated into the development and deployment of products and services. Details can be found at:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&displaylang=en>

Such reports are growing increasingly common throughout the world. These threats alarm consumers and can seriously hinder organizations' competitiveness and damage their reputations.

In response to these trends, organizational leaders have put higher expectations on their IT departments to safeguard the data that is stored, exchanged and processed by the organization's technology framework. At the same time, many IT managers are also feeling pressure to reduce costs and staff time associated with these tasks.

### A Complicated Mix of Laws

Beyond their own internal policies and customer expectations for managing personal information, organizations must also navigate a growing maze of local, national and international privacy and data security laws that often overlap and sometimes even conflict.

In the European Union, for example, individual privacy is described as a "fundamental" right,<sup>3</sup> and the European Commission's Directive on Data Protection limits the transfer of

<sup>2</sup> Source: InformationWeek, "2008 Security Survey: We're Spending More, But Data's No Safer Than Last Year," <http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=208800942>.

<sup>3</sup> Source: "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." *Journal of the European Communities*, November 23, 1995. No L. 281, p. 31.

personal data to nations outside the EU that do not meet their “adequacy” standards for privacy protection.

By contrast, U.S. laws are less uniform. Many states have their own privacy laws that govern specific industries, issues or practices, and a growing number also have data breach notification laws. In addition, an array of federal laws impose rules for financial institutions, healthcare providers, cable operators and telecommunications carriers, as well as rules relating to children’s online privacy, spam, phishing and telemarketing.

And in yet another contrast, regulations in the Asia-Pacific region try to balance privacy protections with economic development and trade goals.

The complexity is even greater in closely regulated industries such as financial services and healthcare, where a company’s best efforts to follow sound internal business processes may inadvertently conflict with regulations in certain countries.

Organizations are left with the daunting and increasingly expensive task of determining which rules apply to their activities, what constitutes a conflict and how to address it. The answers to these questions can be complex: it depends on the type of data involved, the kind of company that collects it, where and how it is collected, and how it might be used.

Consider the challenges facing a consumer goods manufacturer, such as a tire company, that sells products in multiple countries and must collect personally identifiable information about its customers to administer a warranty program. Storing the information centrally on data servers in India might be the most cost-efficient option for this company, yet doing so

### Current Data Handling Practices Create Potential Risks

A 2007 research study by Ponemon Institute LLC in the United States, the UK and Germany found that:

- **Collaboration among security and privacy practitioners in an organization seems to reduce the risk of a compromise or breach of personal information.** 74 percent of organizations with poor collaboration reported one or more data breaches in the preceding 24 months; only 29 percent of those with adequate to excellent cooperation reported a breach.

#### Other key findings:

- **People who collect and use data don’t often consult with security and privacy professionals.** Only 30 percent of marketers said they regularly consult with security and privacy professionals on the collection and use of data, although 78 percent of security and privacy professionals believe they are regularly consulted.
- **Perceptions of collaboration on data protection vary widely within an organization.** 59 percent of privacy and compliance practitioners and 53 percent of security practitioners believe that the safeguarding of personal information is well coordinated within their organizations. In contrast, only 32 percent of people who collect and use data within organizations believe this to be true.
- **Individuals responsible for safeguarding data and those who use it for business purposes differ over the value of good privacy practices.** 50 percent of privacy and compliance professionals and 35 percent of information security professionals cited negligence and mistakes in data use and sharing as the top risks in their organization.

Source: “Microsoft Study on Data Protection and Role Collaboration Within Organizations,” independently conducted by Ponemon Institute LLC, October 2007.

could run afoul of EU regulations—particularly if the data is managed by an outside vendor whose security and privacy policies cannot be directly controlled and assured by the tire manufacturer. Creating separate data centers in each country could be unwieldy and cost-prohibitive, while conforming to the most stringent privacy and security legislation across all countries might prove overly restrictive.

This scenario illustrates some of the challenges in achieving persistent, statutorily compliant protection of sensitive information without diminishing its business value.

## What Is Data Governance?

Data governance is the application of policies and processes within an organization in order to maximize the value of data, manage what data is collected and determine how it is used to advance the organization's goals. Storing data, especially personal information, involves risks that must be appropriately managed through data governance policies and processes. The organization's policies and processes also must address compliance requirements, including the many statutes and regulations that surround data, especially in regulated industries such as the financial and health sectors. Mandatory data retention periods are one example of such requirements.

Data governance, although not a new concept, is gaining renewed interest as organizations grapple with privacy concerns. With growing volumes of personal information to manage, enterprises and governments must balance their goals for using this data to add value to their organization with demands from citizens and policymakers for more accountability and better protections.

This is evident in a 2007 Forrester Research survey, which found that anywhere from 65% of global companies to 90% of small companies with payment card industry (PCI) compliance requirements are still working on becoming compliant.<sup>4</sup> Similarly, an April 2007 survey of 30 security and risk managers attending the Forrester Research Security Forum EMEA found that policy and compliance received the highest average rating when respondents were asked to rank their most important responsibilities.<sup>5</sup>

Fortunately, for many organizations, data governance investments can bring competitive or mission-related advantages in addition to risk reduction. Many of the controls necessary to meet compliance requirements can also serve as operational and financial controls that a savvy manager can employ to improve overall organizational performance. For example, restrictions on the retention of private information that prompt organizations to automatically purge data after a certain period of time can also reduce storage and maintenance costs—which can then drive higher business profits or free up resources for public-sector organizations to improve services to customers.<sup>6</sup> When approached in this way, effective data governance becomes a tool to increase organizational value.

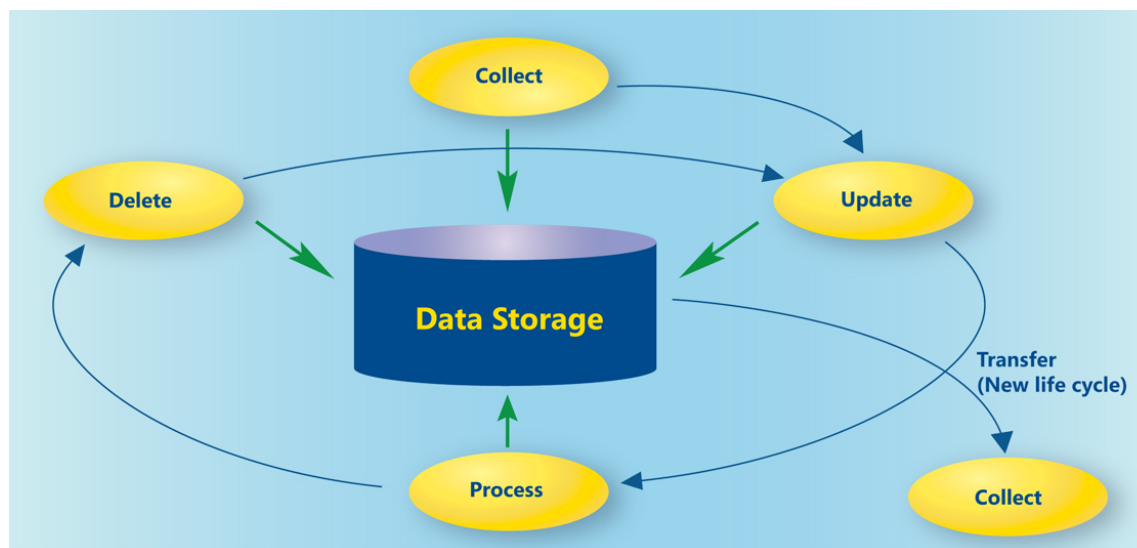
---

<sup>4</sup> Source: Forrester Research, "Confessions of a QSA: The Inside Story of PCI Compliance," September 2008

<sup>5</sup> Source: Forrester Research, "What's Top of Mind for European Security Managers?" May 5, 2007.

<sup>6</sup> Source: Prentice, Robert A., "Sarbanes-Oxley: The Evidence Regarding the Impact of Section 404." *Cardozo Law Review*, forthcoming at SSRN: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=991295](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=991295).

## The Information Life Cycle



Examining how information flows throughout an organization over time and how it is accessed by multiple applications and people for various purposes can help clarify where the organization should deploy technologies to protect personal information. The information life cycle comprises several phases and actions, within which an organization can address specific data governance considerations.

**Collect:** Most organizations collect sensitive personal data in multiple ways—in person, by mail, online—and must establish appropriate controls to help ensure privacy policy compliance, regardless of collection method. This involves setting consistent standards and expectations in contracts with external partners that receive or manage the information, as well as addressing consumers’ desire for greater choice and control regarding how their personal information is collected. Organizations must also consider how their privacy policies will be administered over the lifespan of the data.

**Store:** The task of protecting personal data is relatively straightforward when that data is stored only in a database, but it is far more complex when the information is stored and exchanged within and between organizations in unstructured forms such as e-mail, spreadsheets and text documents. As data in these forms has been increasingly stored on laptops and mobile devices, the risk of data breaches has risen sharply, necessitating more aggressive and sophisticated storage controls.

**Update:** Most data within an organization is updated several times before eventually being deleted. Organizations face challenges in ensuring that only current and accurate data, including personal information, is maintained. Repeated updates can open the door to errors that can compromise the integrity of data.

**Process:** As information becomes easier to share and transmit, it is more frequently subject to processing or use by multiple applications and people—including many outside the organization—as a result of outsourcing agreements and partnerships. In this environment, ensuring that only authorized individuals can access critical

data, and enforcing strict limits on their ability to take data outside the organization (such as on their laptops), are crucial considerations.

Processing can also result in new data—commonly called *audit data*—that describes details such as how the target data was used, when it was accessed and by whom. All of the controls applied to the target data must also be applied to audit data.

**Delete:** With data storage becoming less expensive every day, many organizations have found that spending time deciding which records to delete is more costly than simply keeping it all. However, this practice does not effectively manage the liabilities associated with retaining sensitive information after it has outlived its usefulness. Minimizing an organization's exposure to risk from a data breach by setting a finite lifespan for sensitive data and enforcing policies for its automatic deletion or secure archiving is well worth the effort.

**Transfer:** It is not uncommon for organizations to run reports or extract subsets of data from centralized databases for processing. This is often done using desktop data-mining and analysis tools. Many organizations also routinely transfer large databases to third parties and business partners for processing. Data exported for the purposes of long-term backup or retention in accordance with statutes and regulations is also considered transferred data.

As data is copied or removed from storage as part of the transfer, a new information life cycle begins. Organizations should place as much emphasis on the privacy and integrity of transferred data as they do on the original dataset. In the case of outsourcing, organizations also need to enact appropriate data-handling practices through the organization's privacy and integrity service-level agreements with the outsourcing provider.

## Trustworthy Computing

In 2002, Microsoft Chairman Bill Gates signaled a dramatic shift in the company's strategy: he made providing a secure, private and reliable computing experience for everyone a top company priority. More than six years later, Trustworthy Computing continues to infuse the company's efforts to enhance privacy, safety, security and reliability across all of its products.

Microsoft's commitment to ensuring a trustworthy computing ecosystem has three main areas of focus: technology investments and innovation, leadership and collaboration, and customer guidance and engagement.

### **Technology investments and innovation:**

Microsoft has changed the way it develops software, incorporating security and privacy checkpoints throughout the product development life cycle. To protect against evolving security threats, the company is building technologies that provide layered defenses against malware, spam, spyware and phishing attacks—to name a few. We've also

made important strides in providing easy-to-use services and tools that help customers configure their systems correctly and keep them up to date.

**Leadership and collaboration:** Microsoft works with others in industry, business and government to combat privacy threats and promote best practices. These efforts include formal legal actions and support for law enforcement against spammers and phishers, advocacy for comprehensive privacy legislation, and leadership on a variety of industry-driven privacy initiatives.

**Customer guidance and engagement:** With the understanding that people who use technology also play a vital role in securing the overall computing ecosystem, Microsoft actively engages with customers to help them understand their rights and make educated choices when sharing personal information. For example, Microsoft introduced a "short-layered" privacy notice for many of its online services, providing a clear, concise one-page summary of the company's online privacy practices.

## Data Governance and the Information Life Cycle

Many organizations subscribe to the concepts of Governance, Risk and Compliance (GRC) in addressing issues ranging from meeting myriad statutory and regulatory compliance requirements to achieving basic information security and customer privacy. Unfortunately, these efforts often take place in isolation, with little or no regard for other organizational objectives. Further, the attention to governance is often limited to the IT infrastructure. By also focusing on governance of data, organizations can better implement a comprehensive, integrated and complete GRC strategy, beginning with one of their most important assets—information.

Understanding the information life cycle is vital to an organization's data governance implementation and success. Collection is the beginning of the information life cycle, and it is also the beginning of data governance. Organizations must carefully consider what data actually needs to be collected in order to satisfy their business goals. Once identified, that data can be examined for special handling or storage requirements as defined in legislation or industry regulations—for example, the need to hold certain financial data for a

number of years after use. This information can be documented within the organization's privacy practices along with the need for, and purpose of, the collection and how the data will be used.

A multifaceted approach to data governance involves a combination of policy, people, processes and technology. Once data collection requirements have been identified along with appropriate compliance requirements, organizations can begin to develop appropriate controls to implement data governance and ensure the privacy and integrity of data.

## A Framework for Managing and Protecting Personal Information

Element	Description
Secure Infrastructure	Safeguards that 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	Protecting sensitive personal information in structured databases and unstructured documents, messages and records by means such as encryption so 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

## A Technology Framework for Data Governance

An effective technology-based framework needs the following elements to responsibly protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability. Microsoft is committed to delivering technology advances that contribute to this type of framework for helping organizations protect and manage important personal information.

### Secure Infrastructure

The growing importance of ICT in our work and personal lives underscores the need to make the underlying infrastructure as secure as it can be. Safeguarding and managing sensitive information depends fundamentally on a secure technology infrastructure that protects against malicious software and hacker intrusions as well as misuse of data by rogue insiders.

To help prevent unauthorized disclosure, organizations should build their IT infrastructure using software to continually assess their data risks and then deploy specific security controls that meet the organization's specific needs.

Creating a more secure infrastructure starts with using products and services that are built from the ground up with security in mind. Starting in 2003, Microsoft established a set of strong internal security design and development practices known as the Security Development Lifecycle (SDL). The SDL implements a rigorous process of secure design, coding, testing, review and response for all Microsoft products that are deployed in an enterprise setting, handle sensitive or personal information, or regularly communicate via the Internet. The SDL helps remove security vulnerabilities and minimize the “attack surface” for malicious software and intruders. It also improves system and application integrity and helps organizations manage their networks more securely.

Microsoft provides detailed guidance on the SDL for independent software developers and the worldwide security community to support their efforts to improve the security of their applications and services. More information on the SDL is available at <http://msdn.microsoft.com/en-us/security/cc448177.aspx>.

Microsoft has also implemented the Microsoft Privacy Standard for Development (MPSD). It offers guidance on creating notification and consent procedures, providing sufficient data security, facilitating user access, and supplying controls when developing software products and Web sites. In October 2006, Microsoft published a version of the MPSD known as the Privacy Guidelines for Developing Software Products and Services, which is available at <http://go.microsoft.com/fwlink/?LinkID=75045>.

### **Identity and Access Control**

To reduce the risk of a deliberate or accidental data breach and to help organizations comply with regulatory requirements, Microsoft offers identity and access control technologies that protect personal information from unauthorized access while facilitating its availability to legitimate users. These include authentication mechanisms that verify a user’s identity to help ensure that only valid users can connect to an organization’s system; access controls that determine what resources and data each user is allowed to access; and provisioning systems and management technologies that help organizations manage user accounts across multiple systems and with partners they trust.

One of the challenges facing organizations that operate in a networked world is that the Internet was not designed with a secure identity system in mind. As a result, different identity systems are in use today, each with distinct strengths and weaknesses, and no single system meets the needs of every digital identity scenario.

Because universal adoption of a single identity product is unlikely, Microsoft and the technology industry are working toward a system that offers users of different identity systems a consistent and straightforward user experience. The concept is built on the Seven Laws of Identity, a set of principles that should govern any universally adopted, sustainable identity architecture.

These principles state that the identity framework should:

- Reveal information identifying a user only with that user's consent
- Disclose only the minimum amount of information necessary to facilitate identification
- Be designed so the disclosure of identifying information is limited to parties with a necessary and justifiable place in the identity relationship
- Support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for private entities
- Use and interoperate with multiple identity technologies and providers
- Feature an unambiguous user interface with mechanisms to protect against identity attacks
- Guarantee users a simple, consistent experience

For more information about the Seven Laws of Identity, please visit Kim Cameron's Identity Weblog at <http://www.identityblog.com>.

### **Information Protection**

Legal and regulatory requirements and client expectations regarding management and retention of personal, financial and other business information are greater than ever. As sensitive data is increasingly shared within organizations and across organizational boundaries, it requires persistent protection from interception and viewing by unauthorized parties. Data encryption technologies are one means of achieving this protection. In addition, organizations must ensure that their document management systems and practices can safeguard personal information contained in documents throughout their life cycle.

- **Protecting information through encryption:** Supported by strong identity and access controls, data encryption can help safeguard customer and employee information stored in databases; saved on mobile devices, laptops and desktop computers; and transferred via e-mail and across the Internet. Use of encryption as part of storing, transmitting and disposing of sensitive information greatly reduces the risk of a harmful data breach resulting from an intruder break-in or from a lost or stolen computer or mobile device.
- **Protecting data throughout the information life cycle:** Rights management technologies can be applied to desktop productivity, e-mail and line-of-business applications to help safeguard sensitive information and control how the information is used, through "persistent protection" that extends throughout its life cycle. These technologies can help ensure that sensitive data such as financial reports, product specifications, customer data and confidential e-mail messages do not intentionally or accidentally get into the wrong hands. For example, access to internal documents can be restricted to specific employees within an organization, and users can be prevented from printing them, forwarding them outside the organization, or copying and pasting the text. Users can also apply document retention policies that cause certain content to "expire" after a set amount of time and thereafter be accessible only to the document's creator and to designated data recovery agents.

## **Auditing and Reporting**

To comply with internal policies, government regulations and consumer demands for better control over personal information, organizations can use monitoring technologies to help with auditing and reporting related to data, systems and applications. Technologies for systems management, monitoring and automation of compliance controls can help them verify that system and data access controls are operating effectively and identify suspicious or noncompliant activity.

IT administrators need systems management products that provide tools and information to help ease operations, reduce troubleshooting time and improve planning capabilities.

Such a framework should help administrators to:

- Ensure that computers on their network meet administrator-defined requirements for system health
- Deliver critical business productivity applications reliably and easily to users
- Manage software assets and ensure license compliance by monitoring how installed applications are used
- Reliably deliver software updates across servers, desktops and laptops

## **Principle-Based Application of the Technology Framework**

Beyond the four elements of Microsoft's technology framework for managing and protecting personal information, another important consideration remains: how to apply these technologies in a way that addresses an organization's core objectives.

This is essentially a matter of considering data governance from an architectural perspective, which flows from conceptual principles or value statements down to specific applications of the technologies. Following a set of clearly defined principles for technology design and deployment can help ensure successful protection of both individual and organizational privacy.

Suggested principles include the following:

- **Honor policies throughout the private data lifespan.** Software applications that collect, use and store private data should be controllable through policies and rules.
- **Minimize the risk of data misuse.** Implement applications and systems that guard against unauthorized use of sensitive data.
- **Minimize the impact of data loss.** Safeguard data to ensure that it is not usable when outside of an organization's direct control.
- **Demonstrate the effectiveness of data privacy controls.** Look for data privacy technologies that enable quick response to emerging threats through controls and logs that help uncover problems and determine their source.

## The Role of Government in Data Governance

Governments are uniquely positioned to shape and advance the adoption and implementation of data governance within organizations—and ultimately enhance the privacy protections of their citizens—through thoughtful and precise policy positions and legislation, including the following:

- **Adopt data governance policies and processes.** By adopting data governance policies and processes, governments can demonstrate a commitment to data governance and learn practical lessons about implementation that can be used to form the basis of future policy positions and legislation.
- **Promote data governance.** Governments can use their unique position to promote data governance through academic programs, public-private partnerships, government-sponsored publications and conferences. The insights that governments gain by adopting data governance, when shared freely, are often the most valuable tool in promoting data governance.
- **Implement effective data-retention requirements.** Governments and organizations of all sizes are quickly becoming overwhelmed by the amount of data that they are required to process and store in the course of performing routine business. This problem can be exacerbated by overly broad data retention legislation. Governments can seek a balance between the societal benefits of data retention, including for security and law enforcement, and the risks to privacy that come with long data retention periods.
- **Pass comprehensive data breach notification legislation at the federal level.** Citizens should be informed when their personal information held by governments or organizations is lost or stolen, especially if there is a high likelihood that the information will be used fraudulently or to commit identity theft. Legislation should help balance the rights of citizens to be fully informed with a broader need to limit breach notification to situations where there is a tangible risk of harm. Needless and excessive notification of breaches can decrease consumer confidence in the ICT industry as well as reduce the likelihood that individuals will take proactive steps to protect themselves when they are truly at risk. Federal legislation, aligned with similar laws in other countries, will promote consistency across jurisdictions, simplifying compliance for organizations.

## Conclusion

The loss or theft of personal information held by a government or organization can erode societal confidence in ICT and pose significant risks of fraud and identity theft to individuals. Data governance is a proven strategy that helps governments and organizations to drive broader and more comprehensive GRC practices, which in turn can significantly enhance individual privacy by reducing the likelihood that personal information will be lost, stolen or compromised.

Recommended actions to help organizations successfully implement data governance include:

- **Understand what personal information is being held and its life cycle.** The use of data flow and life cycle diagrams can help an organization understand who has access to personal information

and for what reasons. Understanding the life cycle of personal information can help organizations set appropriate strategies for collection, use, deletion and retention of data.

- **Use the technology framework for data governance to evaluate controls.** The elements of this framework give organizations a reliable basis for examining whether a given technology product offers the necessary functionality to implement technical controls that enhance the privacy of personal information within the organization.
- **Implement data governance controls correctly.** Once controls have been selected, the technology components must be implemented correctly and tested. Any discrepancies between planned controls and implementations must be investigated and rectified.
- **Continuously test and evaluate data governance controls.** Controls should be tested periodically to ensure that they remain effective. Organizations should regularly examine controls, especially if changes have been made in the information life cycle or new technology is implemented, to ensure that they are the best possible controls.
- **Improve communication and collaboration among security and privacy practitioners to reduce the risk that personal information will be compromised.** Recent research has shown that organizations with poor collaboration are more than twice as likely to suffer a data breach as those reporting good collaboration.

Important actions for governments include adopting policy positions and passing legislation in support of data governance; adopting data governance practices themselves and promoting their use; supporting information card technology to enable interoperable identity and access controls; implementing effective data retention requirements; and passing comprehensive data breach notification legislation.