February 2013

Privacy Accountability

Key Points

- Under the principle of accountability for data privacy, an organization is responsible for understanding the risks to individuals that are inherent in processing their personal or sensitive data; for creating policies, tools, and processes to mitigate those risks; and for ensuring that internal privacy controls safeguard personal data.
- Accountability for data privacy is a key Microsoft principle that helps determine how the company and its vendors and partners manage personal information. Each Microsoft business unit is responsible for developing procedures to uphold the company's commitment to protecting personal data.
- Microsoft supports an accountability-based approach to public policy, which permits data to be transferred across international borders without restriction as long as the data exporter remains accountable for protecting the data regardless of its geographic location.

BACKGROUND

Accountability is a long-established principle of privacy and data protection, which was first set down by the Organization for Economic Co-operation and Development (OECD) in the early 1980s. The intent of accountability can be found in the laws of the European Union and EU member states, and is outlined more explicitly in the Canadian Privacy Law (PIPEDA) and the APEC Privacy Framework.

Accountability is best defined as an approach that requires companies that process and store data to analyze and understand the privacy risks this raises for individuals, and take necessary and appropriate steps to mitigate those risks. They must implement programs that align with data protection principles, take responsibility for the safe and appropriate processing and storage of data regardless of its location, and be able to explain how their programs provide the required protections for individuals' data.

The importance of accountability for data protection and privacy has never been greater. Technical innovations related to data collection, analysis, and processing, greater access and flow of data worldwide, and the development of powerful analytic tools have created a situation where more potentially usable data about more people exists than ever before. This new world of accessible, interconnected data requires meaningful privacy safeguards.

Accountability for data privacy has experienced a recent resurgence in privacy policy circles worldwide, with a number of countries developing privacy frameworks that include accountability.

The widespread adoption of a principle of accountability offers many potential benefits. It facilitates the flow of data across international borders, and enables cloud computing by requiring that businesses take responsibility for the management of information regardless of where it resides or is processed.

MICROSOFT APPROACH

- A key Microsoft privacy principle is that of accountability in handling its customers' personal information within the company and with its vendors and partners.
- Each Microsoft business unit is accountable for developing procedures to safeguard data and for assigning specific staff members responsibilities for privacy protection, enforcement, and monitoring.
- Microsoft works with policymakers and other stakeholders to consider how the accountability model might work, how organizations can advance accountability, and what role third-party accountability agents and other validation programs might play in this evolving paradigm.

POLICY CONSIDERATIONS

- Microsoft supports public policies that take an accountability-based approach to data privacy, which permits data to be transferred across international borders without restriction as long as the data exporter remains accountable for protecting the data regardless of where it resides or is processed. This approach holds organizations responsible for protecting data, while still giving them flexibility to accommodate evolving data-transfer needs.
- Microsoft believes that policymakers and other stakeholders should carefully consider how the accountability model might work within legal regimes so as to better protect consumers—while minimizing burdens on organizations and providing clear benefits to those that demonstrate responsible data protection practices, such as through the facilitation of trans-border data flows.
- Microsoft does not believe that regulators should use accountability to impose burdensome external validation mechanisms. For instance, third-party audits or certification schemes can be onerous, expensive, and disproportionate to the potential privacy risks.

Helpful Resources

An overview of Microsoft privacy policies and initiatives
www.microsoft.com/privacy

The Role and Importance of Organizational Accountability in Managing and Protecting Users' Data
aka.ms/accountability-privacy

A collection of accountability-related papers from the Information Policy Centre
aka.ms/accountability-papers