February 2013

Privacy Impact Assessments

Key Points

- A Privacy Impact Assessment (PIA) is defined by European regulators as a “systematic process for evaluating the potential effects on privacy of a project, initiative, or proposed system or scheme and finding ways to mitigate or avoid any adverse effects.”
- Microsoft uses a privacy review process for new services and products that is generally equivalent to what many organizations refer to as a PIA.
- PIA frameworks should be required only where appropriate, and should be flexible enough to enable businesses to develop innovative technologies and tools.

BACKGROUND

Privacy Impact Assessments (PIAs) have emerged in recent years as an important mechanism for assessing and minimizing privacy risk to individuals. The EU PIA Framework Project defines a PIA as a “systematic process for evaluating the potential effects on privacy of a project, initiative, or proposed system or scheme and finding ways to mitigate or avoid any adverse effects.”

Government agencies developed PIAs in the early 1990s in countries such as the United States, Australia, and Canada. In recent years, the use of PIAs has spread to private companies as well as many countries in Europe and Asia.

There are a number of reasons for conducting a PIA, such as those outlined by the U.K. Information Commissioner’s Office: identifying privacy risks to individuals; identifying privacy and compliance liabilities for organizations; protecting an organization’s reputation; instilling public trust and confidence in a product or service; and avoiding expensive resolutions to privacy problems discovered later.

Though PIAs vary widely, a 2007 study by Loughborough University in the United Kingdom found four common elements. Conducting a PIA elicits a prospective identification of privacy issues or risks before systems and programs are put in place or modified, and assesses the impacts in terms broader than those of legal compliance. In addition, PIAs are process- rather than output-oriented, and are systematic.

MICROSOFT APPROACH

Microsoft uses a privacy review process that is generally equivalent to what many organizations refer to as a PIA. The Microsoft privacy review process analyzes and determines the privacy requirements and risks of its products and services early on. This process also provides a series of checks and balances to help ensure that the end products comply with Microsoft’s privacy principles and policies.

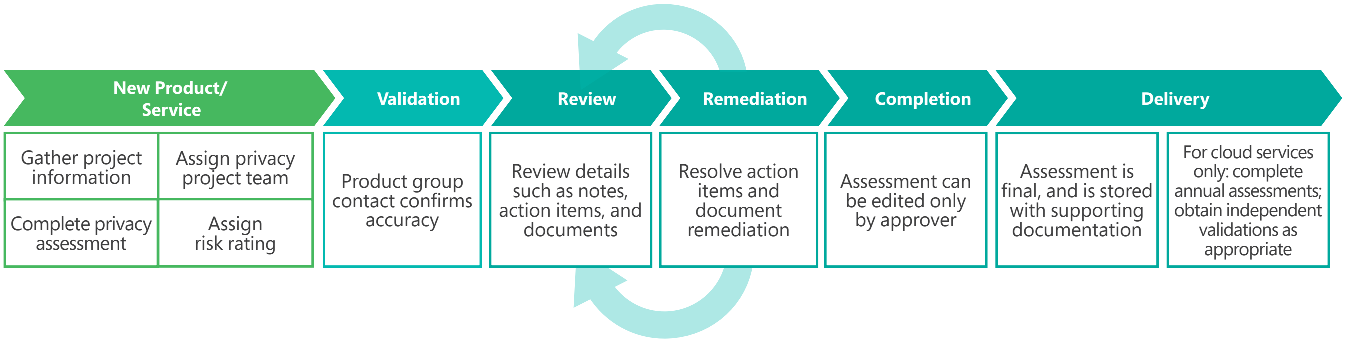
The Microsoft privacy review process follows these phases (illustrated below):

- **Risk assessment.** The first step in Microsoft's typical privacy review process is an assessment that produces a rating of the privacy risk of the product or service.
- **Validation.** The privacy and development teams work together to validate this rating. As the development team designs and builds the product, it may undergo additional privacy assessments.
- **Review and remediation.** During the review and remediation phases, the development team may identify further steps necessary to minimize privacy risks and then implement them. These steps may be repeated many times during product development, until the identified privacy risks have been addressed.
- **Completion and delivery.** Once the product or service is completed, Microsoft conducts a final assessment to determine if all the privacy requirements have been met. If they have, approval is granted. Independent validations and audits may also take place depending on the service.

The privacy review at Microsoft is facilitated through the development and deployment of internal tools that help determine what information is required to complete each review. These internal tools also track the evolution of the product's privacy requirements as it moves from concept to release. They also help the company manage reviews of a wide range of products, including packaged software, Internet services, and web-based marketing campaigns.

POLICY CONSIDERATIONS

- **Selective use.** In some circumstances, it may make sense for regulatory authorities to require the use of PIAs. However, the mandatory use of PIAs for a widespread set of circumstances will likely add unnecessary cost and complexity to the development of products.
- **Flexibility.** PIA frameworks should be flexible and avoid being overly prescriptive to allow businesses to develop innovative privacy technologies and tools. Flexibility means that businesses can adapt their policies and practices to match the contexts in which consumer data is used or shared and the type of relationship they have with the consumer. PIA frameworks should also avoid relying on third parties to conduct PIAs, because the use of third parties works against an environment of transparency and openness between regulators and organizations.
- **Incentives.** One way of encouraging PIAs and robust privacy protection without being overly prescriptive is by offering clear incentives for companies to act responsibly. Accountable controllers could, for example, benefit from less prescriptive requirements or simplified mechanisms to transfer data.
- **Share best practices.** Industry and government should share best practices regarding PIAs and other kinds of privacy review processes. Microsoft makes *Privacy Guidelines for Developing Software Products and Services* publicly available, and has also published *Privacy from the Ground Up*, a white paper that details Microsoft's approach to the many privacy reviews the company conducts annually.



New Product/ Service

Gather project information

Assign privacy project team

Complete privacy assessment

Assign risk rating

Validation

Product group contact confirms accuracy

Review

Review details such as notes, action items, and documents

Remediation

Resolve action items and document remediation

Completion

Assessment can be edited only by approver

Delivery

Assessment is final, and is stored with supporting documentation

For cloud services only: complete annual assessments; obtain independent validations as appropriate

Helpful Resources

An overview of Microsoft privacy policies and initiatives, and a collection of current white papers
www.microsoft.com/privacy

Microsoft Privacy Principles
www.microsoft.com/privacy/principles.aspx

The European Union Privacy Impact Assessment Framework Project
www.piafproject.eu