Privacy

People rely on information technology (IT) in many aspects of their daily lives. And when they use IT, they expect to maintain their privacy and feel certain their personal information is secure.

Many organizations use sophisticated systems to collect, aggregate, and analyze personal information. These trends emphasize the need for companies to protect privacy while providing any-time, any-place functionality.

This constant use of data makes products and services more personalized, convenient, efficient, and widely available. However, it must occur with people's full awareness and understanding, to avoid fears that their data may be vulnerable to misuse. They question whether social networking, location-aware services, and behavioral profiling and targeting threaten their privacy and safety.

Organizational accountability for handling personal information is critical. HP's privacy strategy is based on transparency and choice. We continue to apply an accountability approach to privacy in our business and embed the concept of Privacy by Design in our products and services.

Effective legal frameworks are important, but many privacy laws were created before the widespread use of the Internet and sophisticated tracking technologies. It is often a struggle for regulations to keep pace with emerging technologies. Governments worldwide are taking steps to address this, and we remain heavily involved in shaping these new privacy policies and frameworks. We encourage collaboration between nations and regions to promote relevant, well-defined, and consistent rules.

For more information about our commitment to privacy, read the HP Global Master Privacy Policy.

Leading the way in privacy

- HP placed first among technology companies and second overall in the Ponemon Institute's 2011 Most Trusted Companies for Privacy study among U.S. consumers.
- HP's chief privacy officer, Scott Taylor, testified at a hearing on privacy of the U.S. Senate Committee on Commerce, Science, and Transportation.

HP employees making an impact: Scott Taylor

As HP's chief privacy officer, Scott Taylor and his team work to ensure the personal data of HP customers remains secure by integrating privacy and data protection into HP's processes, products, and services. Learn more about Scott Taylor on page 145.

Approach

It is critical that organizations and their employees are held accountable for the way they handle data and the potential risks they may create. HP's approach is to create a chain of accountability for data privacy and security throughout our processes.

HP teams work together to implement and monitor our privacy program. We also collaborate with external partners to improve privacy protection and related regulations worldwide.

Accountability approach to privacy

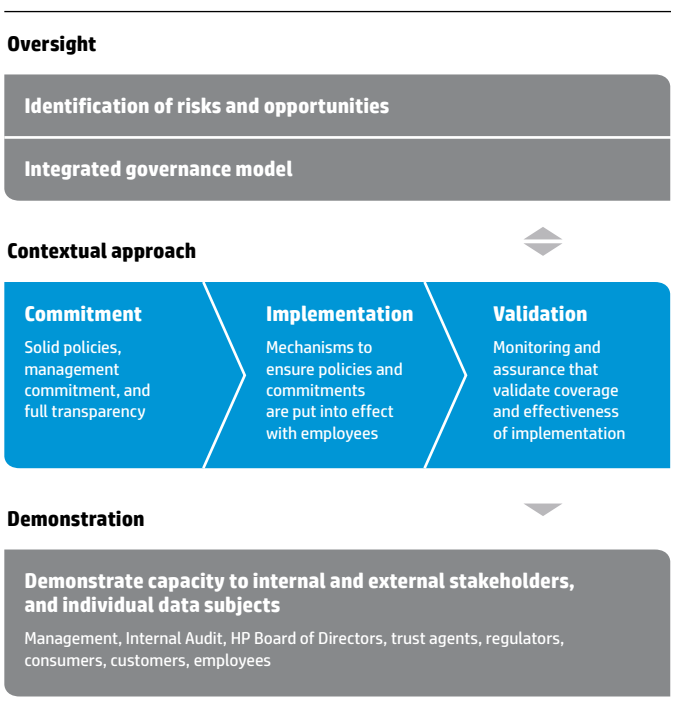
The HP Privacy Accountability Framework (see graphic) is a decision-making model that helps our employees assess and manage the risks associated with collecting and handling personal data. This ensures that HP uses transparent practices and meets our customers' expectations. The framework goes beyond legal requirements, also taking into account our company values, ethical considerations, contractual agreements, and local cultures.

The HP Privacy Advisor tool helps employees apply our privacy standards by guiding them through a privacy impact assessment and risk-management process. All employees who collect or use personal information will use the HP Privacy Advisor tool to assess their projects for compliance.

In 2011, more than 99% of permanent employees completed privacy training as part of our required Standards of Business Conduct course. A specific HP Privacy Advisor module has been developed that will be part of the course in 2012.

Employees in functions that routinely handle personal information, such as human resources, marketing, and client services, receive additional privacy training specific to their role.

HP Privacy Accountability Framework



Privacy and Data Protection Board

The HP Privacy and Data Protection Board (PDPB) is responsible for privacy risk management at HP. It comprises executives from business units and functions throughout the company. The PDPB is part of our overarching Ethics and Compliance governance structure and meets quarterly.

The PDPB assesses privacy risks facing HP each year, and then identifies appropriate ways to mitigate these risks. In 2011, the PDPB identified the following four risk areas: cloud computing, data sharing with partners, data deletion and destruction, and data collected by HP products such as PCs and printers. We are addressing the risks related to cloud computing by working with the HP Cloud Services organization to incorporate Privacy by Design into our cloud offering. We have also added a new PDPB member who represents HP Cloud Services. Deployment of the HP Privacy Advisor tool has helped to mitigate risks arising from data sharing with partners, data collected by HP products, and data deletion and destruction. We have set minimum standards for suppliers handling information on data storage devices returned by HP customers. We audit suppliers to ensure these standards are met.

Monitoring compliance

HP is one of the first companies to have established an internal audit and assurance program to monitor compliance with our privacy policies, and also do so through third-party certifications, dispute-resolution mechanisms (for example, TRUSTe and Better Business Bureau), and customer and employee feedback.

Our Privacy Assurance program assesses internal compliance with our privacy policies and standards, and tracks and mitigates risks and potential noncompliance. The program covers all business units and functions that collect, use, access, or store personal information. In 2011, the Privacy Assurance program received certification from our Internal Audit organization.

All suppliers and third-party vendors who handle HP customer and employee data are contractually bound to comply with the applicable portions of our privacy policies and data security requirements. HP Enterprise Services is responsible for handling clients' personal data and defines our commitments in our client contracts.

Employees and customers can contact our privacy office in more than 30 languages with queries, concerns, or comments. We follow detailed protocols to ensure we handle inquiries and requests effectively, promptly, and appropriately.

Privacy and our products and services

We use companywide product development standards to integrate privacy and data protection into our new products and services—a concept known as Privacy by Design. Our business groups also carry out a privacy impact assessment for new products and services in development using the HP Privacy Advisor tool and consultation with the Privacy Office.

Examples of products and services with privacy features include HP Enterprise Security products, whose Security Intelligence and Risk Management (SIRM) platform protects enterprise customers' applications and IT infrastructures from sophisticated cyber attacks.

In addition, scientists at HP Labs continue to work with our Privacy Office to develop new ways to protect privacy, with a focus on data stored in the cloud. Examples of HP Labs research projects include the long-running EnCoRe research collaboration into easy ways for people to provide and revoke consent for the use of their personal information, and our Trust Domains research into ways to share data in the cloud while maintaining data confidentiality and integrity.

External policy development

New policy frameworks around the world are shifting organizations' legal responsibilities away from simply following rules to demonstrating that they have the capacity to protect privacy and effectively manage risks. HP works closely with regulators, industry, and consumer advocates to contribute to the development of such frameworks.

Though the specific requirements of each framework differ by geography, all are based on well-established and recognized principles such as the Organisation for Economic Co-operation and Development (OECD) privacy principles, so compliance with one makes it easier for organizations to align their practices with the others. This is leading toward greater global interoperability, which benefits organizations and improves consumer protection.

European Union

We remain one of only a few U.S.-based, multinational companies that have been granted Binding Corporate Rules (BCRs) certification by European data protection authorities. BCRs demonstrate that multinational companies have adequate programs and processes in place to uphold the European Directive for Privacy when transferring data between countries. This reduces the effort needed to comply with national laws within the European Union (EU) and assures consumers that they are dealing with a highly reputable organization.

In 2011, we continued our role as one of the Trusted Advisors to the European Commission and data protection regulators as the region's data protection framework is reviewed. We provided a detailed response to the EU's public consultation on cloud computing, emphasizing the need to streamline data protection rules and build trust in the cloud.

Asia Pacific

In 2011, the Asia-Pacific Economic Cooperation (APEC) Ministers of Trade endorsed the implementation of the APEC Cross-Border Privacy Rules (CBPR) system to reduce barriers to information flows, enhance consumer privacy, and promote interoperability across regional data privacy regimes. This includes a commitment to implementing the CBPR system as one step toward further opening markets and facilitating regional trade. HP remains actively involved with the implementation of the CBPR system.

Latin America

We are providing guidance to several Latin American countries as they introduce new privacy regulations. For example, HP has been working with the Ministry of Commerce and business groups in Colombia to contribute to the base law and secondary regulations and provide industry comments. When implemented, this will be the first of a "new generation" of laws that integrates traditional concepts of privacy with innovative new approaches such as binding co-regulatory programs and binding corporate rules. HP has provided similar consultation on the legislative process in Mexico, where new legislation came into effect in 2011.

Global advocacy

Our Privacy Office has continued to work with international regulators and industry groups through the Center for Information Policy Leadership on a multiyear project to define what it means for a company to be accountable for its privacy practices. The first phase of this work identified the essential elements of accountability and the second phase defined ways to measure accountability. In 2011, the third phase, sponsored by the Spanish Data Protection Authority, described the governance model companies should adopt to implement accountability in the marketplace.