Protecting your data

EY's approach to data privacy and information security

EY

Building a better working world

Overview

Digital networks are a key enabler in the globalization of business. They dramatically enhance our ability to communicate, share and store information and connect with colleagues and clients. New technologies bring new capabilities and, perhaps, a greater risk of non-controlled data disclosure. This reality has prompted a number of regulators to increase data privacy constraints, including limits on international transfers of personal data, and specify information security requirements designed to protect the confidentiality, integrity and availability of business and personal information.

At EY, we believe that a strong business reputation depends on a robust data privacy and information security program.

EY views data privacy and information security as fundamental components of doing business. We are committed to protecting information assets, personal data and client information. We believe that a solid data privacy and information security program is an essential component of a leading professional services organization.

The purpose of this document is to summarize our approach to data privacy and information security. It provides an overview of how we secure client information and our systems housing this information, keeping in mind that the specifics of these measures may vary depending on the service and the applicable country regulatory requirements.

Our data privacy and information security program and practices are focused on sharing information appropriately and lawfully, while providing confidentiality, integrity and availability.

A well-articulated security and privacy strategy

Our ability to provide seamless, consistent, high-quality client service worldwide is supported by a well-articulated data privacy and information security strategy. We protect information assets, personal data and client information whenever and wherever they are created, processed, transmitted or stored. We develop and maintain ongoing compliance with applicable domestic and international regulatory standards.

The implementation of our data privacy and information security program and practices is managed by two distinct yet aligned groups: the Global Data Privacy Network and the Information Security organization. Their mission is to protect the information assets of EY and its clients from unauthorized collection, retention, use, disclosure, modification or destruction. This is accomplished through appropriate policies, procedures, guidelines and technical security architecture.

Our Global Data Privacy Network and Information Security organization are aligned under global priorities which are consistently implemented worldwide within the EY organization. This provides a single, cohesive vision around the protection of our information assets, personal data and client information.

Key initiatives

Global data privacy policy

Our global data privacy policy addresses the issues raised by modern data management tools and systems. We apply a common set of personal data management principles to all our member firms, providing a framework for processing personal data in compliance with their local privacy laws and professional standards, as well as their own internal policies.

The following are the principles of our global data privacy policy:

- We protect personal data using appropriate physical, technical and organizational security measures.
- We process, store and disclose personal data only for legitimate business purposes.
- We make sure our contracts with third-party processors contain terms that confirm data is managed according to the same standards we implement across the enterprise.
- We give additional attention and care to sensitive personal data, making sure we respect local laws and customs.
- We've established appropriate measures to ensure personal data remains accurate, complete, current, adequate and reliable.
- Where applicable, we provide notice to individuals with whom EY member firms engage, advising them of the purpose for which we are processing their personal information.

International intra-group data protection agreement

All EY member firms that process personal data have entered into an international intra-group data protection agreement (IGA). The purpose of the IGA is to set out the relationship between these entities with respect to international transfers of personal data. The IGA is consistent with the standards established by the European Union Directive 95/46/EC on the protection of personal data. The IGA legitimizes transfers of personal data between member firms around the world, in compliance with international standards and local data privacy laws.

When necessary, in addition to the IGA, further initiatives are undertaken. As an example, our US member firm is registered with the U.S. Department of Commerce for the Safe Harbor certification, which aims to harmonize data privacy practices in trading between the US and the stricter controls of the European Union Directive 95/46/EC.

Binding corporate rules

EY is working toward introducing binding corporate rules (BCR) to the existing global personal data privacy program to legitimize international data transfers. Our BCR policy is currently being reviewed as part of the European Data Protection Authorities (DPA) Mutual Recognition process and, once finalized, will be available on our global website as a public statement of EY's commitment to good data management practices.

Global code of conduct

We hold our professionals to the applicable professional and technical standards and require strict adherence to our global code of conduct. These principles are publicly available for viewing on our global website (http://www.ey.com/GL/en/Home/Global-Code-of-Conduct) and represent binding standards that apply to all member firms globally.

The global code of conduct is based on a comprehensive behavioral and ethical framework. It guides the daily decisions made by all our people, regardless of their individual role, position or member firm. It demands that employees respect and protect both personal and confidential information obtained from, or relating to, EY, our clients or third parties.

Data privacy and information security awareness

As attack methods change, so must the information, guidance and training we offer our people. Raising awareness of threats to data privacy and information security is an ongoing and dynamic process. It is one that EY takes very seriously, and it is reflected not only in specialized formal training for employees in each of our service lines, but in numerous other activities to raise awareness within the entire global EY population.

Information security strategy and mindset

Our global information security program is designed to drive and promote the confidentiality, integrity and availability of our personal and client information assets. We support this effort through our global information security policy in concert with our focus on data protection technologies. We implement technical security controls to manage data in accordance with privacy law, regulatory requirements and generally accepted security principles.

We are proactive in securing and properly managing confidential and personal information through our ISO 27002–based information security program, which includes:

- Appropriate policies, standards, guidelines and program management
- Strong technical security controls
- A security compliance program involving security reviews, certifications and audits
- A clearly defined security strategy and road map that consider the following:
  - Data privacy: legal, regulatory and procedural requirements
  - Business: mandated procedures and requirements
  - Technology: policies, standards and procedures
  - External threats: changes to the security threat landscape
- A security incident management program to effectively control and remediate security-related incidents

Disaster recovery program

EY's continued commitment to protecting organization and client data is demonstrated through our disaster recovery capabilities.

We are committed to protecting our people, facilities, infrastructure, business processes and data during and after a catastrophic event. The response and system recovery to our critical business environment has been carefully planned and tested to demonstrate that our most critical business applications are readily available in the event of a declared disaster.

EY's disaster recovery methodology incorporates the following:

- Mission-critical disaster recovery plans built on industry-leading standards
- Support from certified disaster recovery planners
- Regular testing of disaster recovery plans to ensure operational readiness

About our information security policy

Our multifaceted and detailed security program is anchored by our global information security and personal conduct policies. This enables us to consistently apply appropriate security standards, controls and guidance.

Our information security policy and its supporting standards and controls are continually reviewed, vetted and approved by senior management. We conduct these reviews to confirm that the material remains timely and accurate, and that it correlates to legal or regulatory requirements applicable to our organization. This policy is built upon the internationally accepted standards for security program management, ISO 27001/2.

Mandatory and recommended security policy statements span nearly a dozen widely recognized information security areas, including but not limited to:

- Access control
- Asset management: classification and control
- Communications and operations management
- Human resources security: personnel
- Information systems acquisition, development and maintenance
- Physical and environmental security

About our information security technology controls

Our approach to information security does not rely solely upon written security policy or standards. We also maintain the confidentiality, integrity and availability of information through the protection of our technology resources and assets. Measures include, but are not limited to:

- Full disk laptop/desktop encryption
- Removable media encryption tools (e.g., USB "thumb" drives)
- Desktop/laptop firewall
- Antivirus/anti-malware software
- Multi-factor authentication solutions
- Automated patching and security vulnerability assessments
- Strong physical, environmental and perimeter controls
- Intrusion detection and prevention technologies

In addition, we invest considerable time and resources into future-state security technologies through our technology security strategy. We align our information security strategy to our technology product road map and maintain close association with our technology service offerings. This properly positions us to address security issues that might otherwise threaten the confidentiality, integrity or availability of our technology resources.

At EY, we believe that a strong business reputation depends on a robust data privacy and information security program.

Compliance and audit

We have a strong data privacy and information security program. We maintain an effective governance function, and we conduct compliance reviews through formal audit exercises. We manage compliance with data privacy and information security obligations by executing the following reviews and programs.

Security certification process

We rely on our applications and systems to service, manage and store our information and that of our clients. All applications and systems are subject to our security certification process, where they are reviewed by information security professionals prior to implementation. This is to confirm that the applications and systems have been developed in accordance with our information security policy and secure application development standards.

The security certification process is recursive in nature and incorporates risk assessment, documentation reviews, penetration testing and vulnerability assessments. It is applied to any application or system used to create, store or manage information on behalf of EY. This process helps us to maintain the confidentiality, integrity and availability of our information and that of our clients.

Global privacy impact assessments

We conduct regular, thorough privacy impact assessments (PIAs) of our global applications and business initiatives that handle personal information. Each PIA reviews the application or initiative against global standards and, where necessary, provides advice to mitigate data privacy and confidentiality risks.

Following a PIA, a list of data privacy and confidentiality recommendations, with detailed guidelines, is prepared for all users and administrators of that system. This detailed assessment satisfies data transfer requirements for EY member firms in the European Union, as established by the local regulators in the region.

The appropriate policies and guidance have been published to enable all new global applications to be designed and developed according to data privacy standards driven by the global systems and process review.

Information security self-assessments

Information security self-assessments are a core element of our annual compliance and review activities. IT managers responsible for development and operations of our global technology services must indicate compliance with relevant security policy statements or standards. Information security self-assessments are also completed by managers of data centers and other facilities that house or process client data. All findings are documented through our governance, risk and compliance processes.

This enables us to gauge the efficiency, effectiveness and completeness by which information security controls are implemented. It also enables us to evaluate information security controls in terms of their implementation and continued management, as required by our global information security policy.

Information security audits

To obtain a more complete view of our information security compliance, our global technology products, services and data centers are subject to audits. We conduct several forms of audit:

- Annual ISAE 3402 audits of our three global data centers in the US, Germany and Singapore, in which our security controls are audited and verified by an independent third-party auditor
- Network vulnerability scans, which focus on the technical aspects of the global information security policy, such as patch management, application security and infrastructure security
- Foundation audits, which review technical controls and build processes of components such as operating systems, databases and infrastructure
- On-site field audits, which include interviews with key management personnel, detailed site walk-throughs, documentation reviews and network vulnerability scans. These on-location investigations are the most significant and detailed form of audit, assessing compliance with all aspects of global information security policy

Information security compliance audit findings are compiled and vetted by senior management. These findings are weighed against the results from the initial self-assessment exercise, and any identified gaps are included in the final report. Corrective action plans are determined and accepted, should they be required.

Information security exceptions

If an issue cannot be managed through a corrective action plan, an exception process is employed to generate the necessary dialogue around the issue. The exception process includes, but is not limited to, a formal approval process, regular reviews of each exception and a security assessment with an assigned risk rating. Compensating controls typically accompany any approved exception to help properly mitigate risks that may arise as a consequence of the modification.

This exception process confirms that exceptions and any subsequent corrective actions are properly documented, managed and readdressed at a future date.

Summary

EY secures information assets for our clients through the use of an integrated data privacy and information security strategy:

- We align our information security governance with our data privacy governance to provide a consistent, cohesive vision around the protection of our information assets, personal data and client information.
- We subject our global applications and systems to both data privacy impact assessments and security certification reviews, which enable a robust, consistent approach in deployment and operation.
- We protect personal data within our network using appropriate physical, technical and organizational security measures.
- We provide assurance that our contracts with third-party processors contain provisions that are commensurate with our own policies, practices and controls to confirm your data is managed properly and securely, in accordance with legal and regulatory requirements.

Clients and individuals rightfully demand accountability from any organization handling their personal and confidential data. We understand the importance of taking appropriate steps to safeguard information assets and are committed to protecting information relating to our clients and to our people.

If you have any questions or require further information on the ways in which we protect you and your business, please contact your EY representative.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG No. CN0031

ED none

ey.com