Protecting your data
EY’s approach to data privacy and information security
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, with new capabilities, an increased risk of uncontrolled data disclosure. This reality has prompted a number of regulators to increase data privacy constraints, including limits on international cross-border transfers of personal data, and to 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 maintain an effective governance function and 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.

Elements of our data protection framework

**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 has successfully applied for binding corporate rules (BCR) to the existing global personal data privacy program to legitimize international data transfers. Our BCR policy is 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.

---

**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 local privacy laws and professional standards as well as their own internal policies. Our global data privacy policy is based on the following principles:

- We protect personal data using appropriate physical, technical and organizational security measures.
- We process, store and disclose personal data only for legitimate business purposes.
- 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, and respect local laws and customs.
- We have established appropriate measures to maintain personal data as 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.
Global information security policy

Our information security policy and its supporting standards and controls are continually vetted by senior management to confirm that the material remains timely and accurate, and that it correlates to legal or regulatory requirements applicable to our organization. Mandatory and recommended 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 security
- Human resources security: personnel
- Information systems acquisition, development and maintenance
- Physical and environmental security
- Risk assessment
- 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, including a Cyber Defense Critical Vulnerability Response Program
Technical security 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 (server, endpoint, gateway)
- Multi-factor authentication solutions
- Automated patching and security vulnerability assessments
- Strong physical, environmental and perimeter controls
- Intrusion detection and prevention technologies
- Monitoring and detection systems

In addition, we invest considerable time and resources into future-state security technologies. 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.

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, applications and data during and after a catastrophic event. The response and system recovery to our critical business applications has been carefully planned and tested. EY’s disaster recovery methodology incorporates the following:

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

Vendor assurance program

Our vendor assurance program aligns with EY’s vendor management due diligence process to cover third-party activities related to information security, procurement, contracts, data privacy and independence, including:

- Evaluation of prospective vendors for compliance with EY’s ISO 27001/2 aligned global policies and controls
- Due diligence reviews, including preparation of risk ratings and findings
- Mitigation of risk findings
- Support in vendor selection and contract negotiations

We use industry-standard security assessments to evaluate inherent and residual risk across information security, compliance and other third-party risk categories such as data classification, data location, access and data transmission type.

Alignment of our global data privacy and information security priorities enables a single, cohesive vision around the protection of our information assets, personal data and client information.
Compliance and audit

We have a comprehensive 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
Prior to implementation, all applications and systems are subject to our security certification process to confirm that they have been developed in accordance with our information security policy and secure application development standards.

The security certification process 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.

Control effectiveness assessments
To verify controls are implemented and operating effectively, EY performs a number of assessments of control effectiveness, including:

- Network and application vulnerability assessments, which focus on the technical aspects of the global information security policy, such as patch management, application security and infrastructure security
- Operating effectiveness assessments, which review technical controls and build processes of components such as operating systems, databases and infrastructure
- Ongoing operational monitoring of control effectiveness, to validate that the security controls are implemented and configured appropriately

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 SOC2, Type II attestation conducted by an independent third-party auditor, which encompasses the security, confidentiality and availability trust principles and covers our three global data centers in the US, Germany and Singapore
- 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. 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 used to review the risks associated with the issue and explore alternatives. The exception process includes a formal approval process, regular reviews of each exception and a security assessment with an assigned risk rating. Compensating controls typically accompany approved exceptions 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 revisited 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.
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.

© 2015 EYGM Limited.
All Rights Reserved.

EYG No. CN0038
1502-1396363 NY
ED none

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com