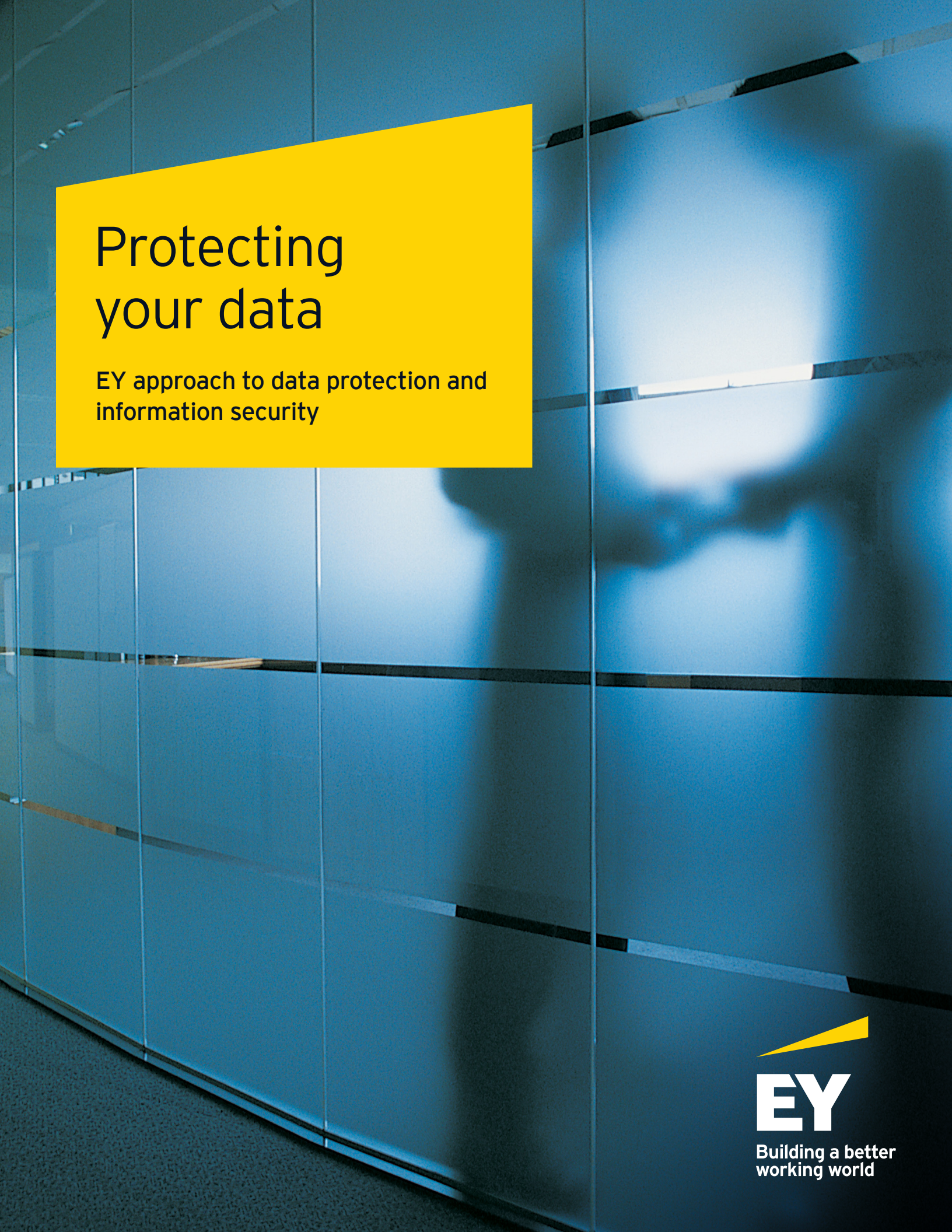

Protecting your data

EY approach to data protection and information security

Building a better working world

The EY organization believes that a strong business reputation depends on a robust data protection and information security program.

We view data protection and information security as fundamental components of doing business. We are committed to protecting information assets, personal data and client information. We believe that solid data protection and information security programs are essential components of a leading professional services organization. The purpose of this document is to summarize our approach to data protection and information security and to provide an overview of how we secure client information and our information systems that support it. The specifics of these measures may vary depending on the services performed and applicable country regulatory requirements. Our data protection and information security programs and practices are focused on sharing information appropriately and lawfully while preserving confidentiality, integrity and availability.

A well-articulated information security and data protection strategy

The EY teams' ability to provide seamless, consistent, better-quality client service worldwide is supported by a well-articulated data protection and information security strategy. We protect information assets, personal data and client information whenever and wherever they are created, processed, transmitted or stored. We also maintain effective governance and ongoing compliance with applicable domestic and international regulatory standards.

The implementation of our data protection and information security programs and practices is implemented and managed by two distinct yet aligned groups: the Global Data Protection network and the Global Information Security organization. Their mission is to protect the information assets of our organization and EY clients from unauthorized collection, retention, use, disclosure, modification or destruction. This is accomplished through appropriate policies, standards, guidelines and supporting procedures, technological and administrative controls, and ongoing training and awareness efforts.

The EY Global Data Protection teams and Global Information Security organization are aligned under global priorities that are implemented worldwide within the EY organization. This provides a single, cohesive vision around the protection of information assets, personal data and client information.

Our data protection framework
Our data protection framework is based on relevant principles of law (including the EU General Data Protection Regulation (GDPR)), other regulatory requirements, and relevant professional standards. It demonstrates the commitment of all EY member firms to safeguard personal data and confidential data (including client data) based on the following principles:

- Lawfulness, fairness and transparency: use data in ways that are ethical, reasonable, clearly communicated and lawful
- Purpose limitation: only using data for defined and approved uses
- Data minimization: collecting and processing no more data than is required for the purpose
- Accuracy: verifying that data remains accurate and is of sufficient quality for the proposed purpose
- Storage limitation: retaining data only for as long as required to meet the purpose it was collected for
- Integrity and confidentiality: verifying that data is kept secure and confidential and access is controlled on a strict "need to know" basis
- Accountability: being able to demonstrate compliance with the data protection principles, in accordance with EY Global Data Protection & Confidentiality policy and Code of Conduct
- Sensitive information: taking additional care when processing sensitive personal data or sensitive client information
- Third-party processors: verifying that third parties who process personal data or confidential data including client data on behalf of the EY organization have adopted a data protection framework that provides appropriate protection of such data and that contracts with such third parties contain data protection terms in accordance with applicable laws

Elements of our data protection framework

International data transfers
International personal data transfers are strictly regulated by key data protection laws and regulations (such as European data protection law). Various data protection laws around the world prohibit the offshore transfer of personal data unless the organization transferring such data has implemented appropriate safeguards. EY teams use approved data transfer mechanisms to comply with data protection laws. We are also mindful of the ruling of the Court of Justice of the European Union (CJEU) in Schrems II when transferring European personal data to countries outside the European Economic Area without a comprehensive legislative approach to data protection such that they are not deemed by the EU to provide an adequate level of protection for individuals' data privacy rights.

- EY teams conduct data transfer impact assessments of local laws and practices and include appropriate supplementary measures to verify adequate protection of personal data, as necessary.
- EY teams have identified binding corporate rules (BCRs) for controller as well as processor activities as a mechanism to permit the international transfer of personal data between EY member firms. BCRs help enable us to transfer personal data seamlessly within EY member firms, facilitating cross-service line teaming. These BCRs, which have been applied across EY member firms across the globe are published at ey.com/bcr.
- EY member firms make use of approved standard contractual clauses (SCCs) in contracts with clients and third parties where appropriate.
- Ernst & Young LLP, US, and its affiliated US entities, adheres to the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework published by the U.S. Department of Commerce. To learn more, see Ernst & Young LLP EU-US Data Privacy Framework Privacy Statement.

Alignment of global EY data protection and information security priorities supports a single, cohesive vision concerning the protection of information assets, personal data and client information.

Training and awareness programs
As attack methods change, so must the information, guidance and training we offer EY people. Raising awareness about threats to data privacy and information security is an ongoing and dynamic process. It is one that we take very seriously, which is reflected not only in mandatory training updated regularly for professionals in each EY service line, but also in numerous other activities to drive awareness within the entire global EY population.

EY Global Information Security Policy

Our Information Security policy and its supporting standards and controls are continually vetted to confirm that the material remains timely and accurate and that it correlates to legal and regulatory requirements applicable to us. In alignment with recognized frameworks, such as ISO 27001, 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 security acquisitions, development and maintenance
- Physical and environmental security
- Risk management

Technical security controls
Our approach to information security does not rely solely upon a written security policy or standard. 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:

- Desktop and laptop full disk encryption
- Removable media encryption tools
- Desktop and laptop firewalls
- Antivirus and anti-malware software
- Multifactor authentication approaches
- Automated patching and security vulnerability assessments
- Strong physical, environmental, network 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 roadmap and maintain a 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.

Global Code of Conduct

We hold our professionals to the applicable professional and technical standards and require adherence to the EY Global Code of Conduct. These standards, which are publicly available for viewing on the EY global website (ey.com/en_gl/global-code-of-conduct), represent binding principles that apply to all member firms globally. The EY Global Code of Conduct is based on a broader behavioral and ethical framework. It guides the daily decisions made by all EY people, regardless of their individual role, position or member firm. It also requires that professionals respect and protect both personal and confidential information obtained from, or relating to, the EY organization, EY people, EY clients or third parties.

Information Security

Business continuity and disaster recovery
Our continued commitment to protecting the EY organization and client data is demonstrated through our disaster recovery and business continuity capabilities, in alignment with ISO 22301. We are committed to protecting EY people, facilities, infrastructure, business processes, applications and data before, during and after a catastrophic event. The disaster response and system recovery procedures for our critical services applications have been carefully planned and tested. Our disaster recovery and business continuity methodologies incorporate the following:

- Business impact assessments
- Mission-critical disaster recovery plans built on industry standards
- Support from certified disaster and business continuity recovery planners
- Regular testing of disaster recovery and business continuity plans to verify operational readiness

Supplier risk assurance program
This program aligns with our supplier management due diligence processes to cover third-party activities related to information security, procurement, contracts, data protection and independence, including:

- Evaluation of prospective suppliers for compliance with our ISO 27001/2 aligned global policies and controls
- Due diligence reviews, including preparation of risk ratings and findings
- Help in mitigation of risk findings
- Support in supplier selection and contract negotiations

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

Security strategy and mindset
Our multifaceted security program is anchored by information security and personal conduct policies across the globe. It is designed to drive and promote the confidentiality, integrity and availability of our personal and client information assets. We support this effort through data protection technologies applied in accordance with applicable privacy laws and regulatory requirements, as well as the ISO 27001/2 internationally accepted standards for security program management.

Our organization is proactive in securing and properly managing confidential and personal information through our ISO27001/2 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 roadmap that consider the following:
  - Data protection: 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

Compliance and audit

EY teams have global data protection and information security programs. We maintain an effective governance function and review compliance through formal audit exercises. We support compliance with data protection 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 policies and secure application development standards.

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

Privacy and confidentiality impact assessments
EY teams that develop or implement systems or tools that handle personal data or client information must liaise with data protection teams to perform a privacy and confidentiality impact assessment (PIA). A PIA reviews the system or tool 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 is prepared for all users and administrators of that system or tool. This detailed analysis includes a review of any cross-border data transfers to confirm these meet applicable legal and regulatory requirements.

We utilize a broad suite of policies and guidelines to assist the deployment of systems and tools in accordance with applicable data protection standards and requirements.

Control effectiveness assessments
To verify that controls are implemented and operating effectively, we perform several 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 security controls are implemented and configured appropriately

Information security audits
To provide EY teams with a more complete view of information security compliance, EY global technology products, services and data centers are subject to audits. EY teams conduct several forms of audit:

- Independent third-party compliance audits against ISO 27001 to certify the Information Security Management System employed within our three global data centers in the US, Germany and Singapore and local data rooms
- Independent third-party compliance audits against ISO 27017 to certify the information security controls within the cloud-based EY Fabric client technology platform computing environment
- Independent third-party compliance audit against ISO 22301, which encompasses the elements of the EY global business continuity management system
- Annual SOC 2, Type 2, attestation conducted by an independent third-party auditor, which encompasses the security, confidentiality and availability principles and covers our three global data centers in the US, Germany and Singapore, local data rooms, and the third-party cloud-based EY Fabric, the client technology platform
- Annual ISAE3402/ SOC1, Type 2 attestation of our three global data centers in the US Germany and Singapore, local data rooms, and the third-party cloud-based EY Fabric, through which our security controls are tested and verified by an independent third party
- Network vulnerability scans that focus on the technical aspects of our EY 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 – the most significant and detailed form of audit assessing compliance with all aspects of our EY 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. This 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 because of the modification. This exception process confirms that exceptions and any subsequent corrective actions are properly documented, managed and reviewed at least annually.

Summary

We secure information assets of EY clients by adhering to the integrated data protection and information security strategy:

- Subjecting the global applications and systems to a variety of assessments and reviews, including data privacy impact assessments, security certification reviews and business impact assessments, which support a robust consistent approach in deployment and operation.
- Protecting personal data within the EY network using appropriate physical, technical and organizational security measures.
- Contracts with third-party processors contain provisions commensurate with our policies, practices and controls and confirm that client 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 EY clients and EY people.

For any additional questions or further information on how EY protects clients and their business, please contact an EY representative.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

005757-24Gbl | ED None

ey.com