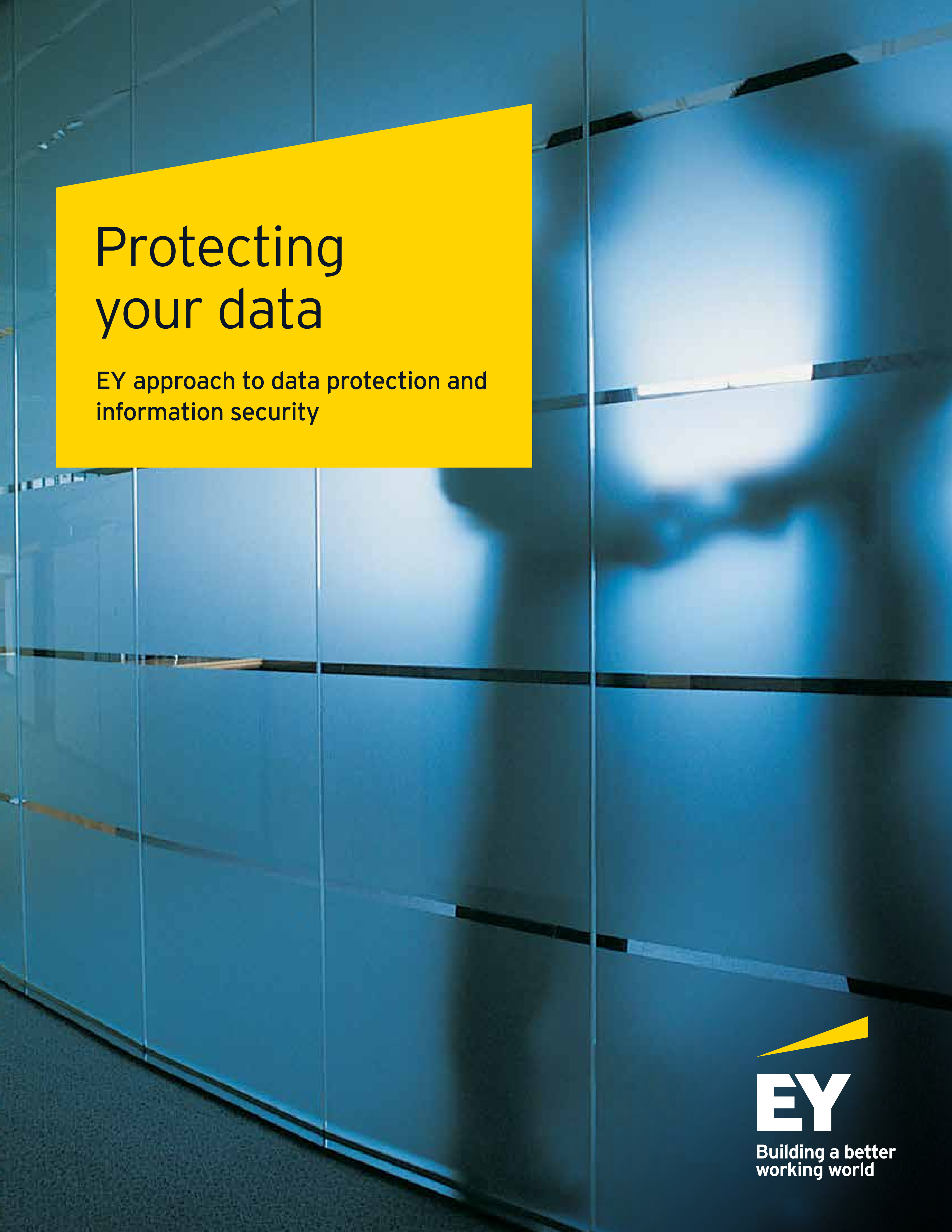


Protecting your data

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.

EY views data protection and information security as fundamental components of doing business. EY teams are committed to protecting information assets, personal data and client information. EY believes 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 the EY approach to data protection and information security and to provide an overview of how EY people secure client information and the EY information systems that support it. The specifics of these measures may vary depending on the services performed and applicable country regulatory requirements. EY 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, high-quality client service worldwide is supported by a well-articulated data protection and information security strategy. EY professionals protect information assets, personal data and client information whenever and wherever they are created, processed, transmitted or stored. EY teams also maintain effective governance and ongoing compliance with applicable domestic and international regulatory standards.

EY data protection and information security programs and practices are 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 the EY organization and EY clients from unauthorized collection, retention, use, disclosure, modification, or destruction. This is accomplished through appropriate policies, standards, procedures, guidelines, 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.

EY data protection framework
Based on the principles of the EU General Data Protection Regulation (GDPR), the EY data protection framework addresses the issues raised by modern data management tools and systems. EY teams apply a common set of personal data management principles to all EY member firms, providing a methodology for processing personal data in compliance with GDPR, local privacy laws and professional standards, as well as EY member firm internal policies. The EY data protection framework is based on the following principles:

- Protect personal data using appropriate physical, technical and organizational security measures. These measures are designed to facilitate compliance with data protection requirements by design and by default.
- Process, store and disclose personal data only for legitimate business purposes.
- Verify contracts with third-party processors require that data is managed in accordance with the same standards EY teams implement across the enterprise. Contracts with third-party processors contain terms that confirm data is managed in accordance with EY standards.
- Give additional attention and care to sensitive personal data.
- Implement identified appropriate measures to keep personal data accurate, complete, current, adequate and reliable.
- Retain personal data in a form that permits identification for as long as necessary.
- Where applicable, we notify individuals with whom EY member firms engage, advising them of the purpose for which EY processes their personal data.
- Keep a record of categories of processing activities carried out. Processing activities likely to result in a high risk to the rights and freedoms of natural persons will be subject to a data protection impact assessment.

Elements of EY 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. EY teams 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 helped establish 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 enable EY to transfer personal data seamlessly within EY member firms, facilitating cross-service line teaming. These BCRs, which have been applied across EY 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.

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 EY people are offered. Raising awareness about threats to data privacy and information security is an ongoing and dynamic process. It is one that EY teams 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

This 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 and regulatory requirements applicable to EY teams. Mandatory and recommended policy statements span nearly a dozen widely recognized information security areas, including, but not limited to:

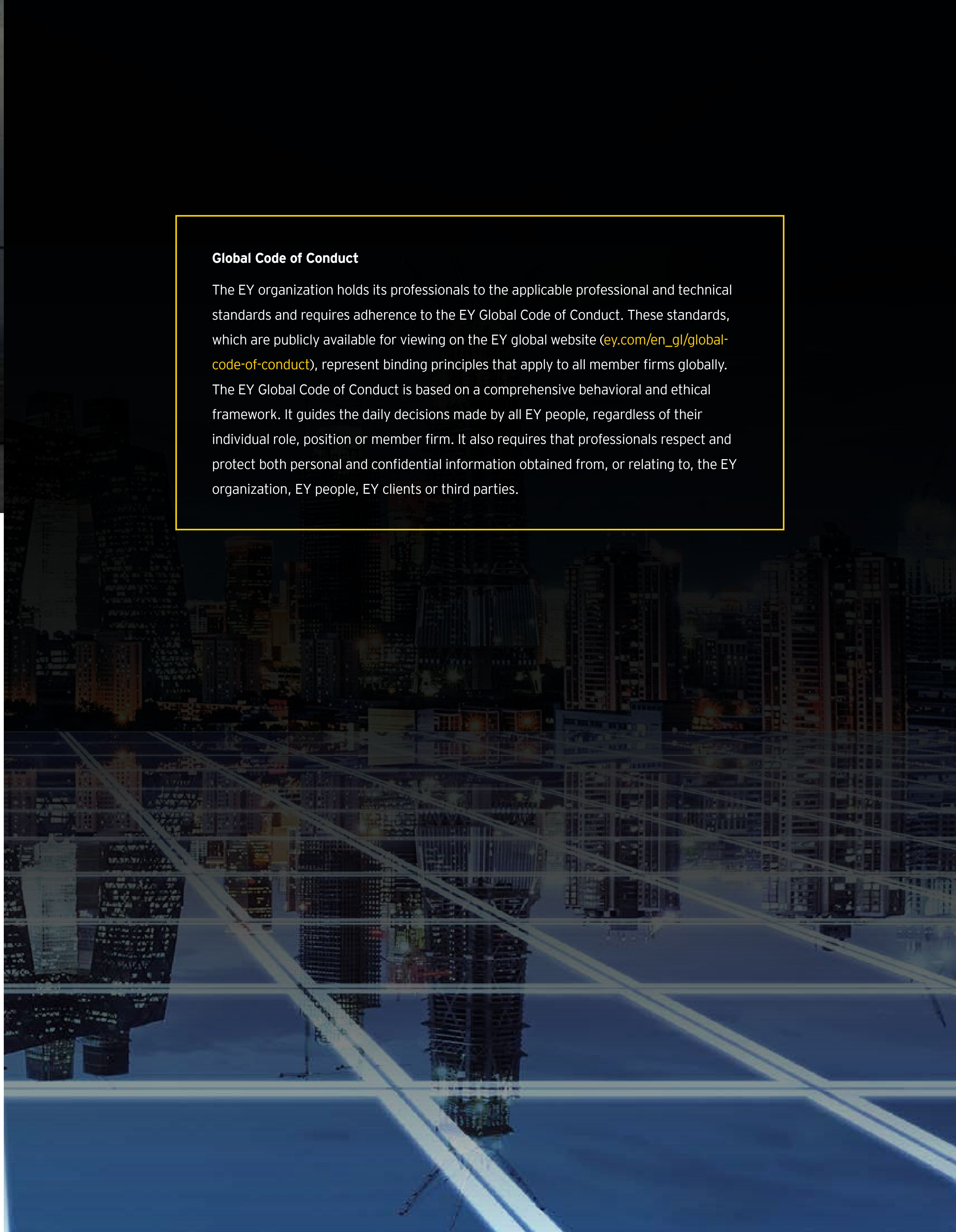
- Access control
- Asset management: classification and control
- Communications and operations security
- Human resources security: personnel
- Information systems acquisition, development and maintenance
- Physical and environmental security
- Risk assessment

Technical security controls
The EY approach to information security does not rely solely upon a written security policy or standard. EY teams also maintain the confidentiality, integrity, and availability of information through the protection of EY 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, EY people invest considerable time and resources into future state security technologies. The EY aligns the information security strategy to the organization's technology product roadmap and maintains a close association with EY technology service offerings. This properly positions the EY organization to address security issues that might otherwise threaten the confidentiality, integrity or availability of our EY technology resources.

EY teams offer tools designed to help collaborate with EY clients and to securely and reliably transfer and store data.



Global Code of Conduct

The EY organization holds its professionals to the applicable professional and technical standards and requires 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 comprehensive 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.

Data protection

Business continuity and disaster recovery
Continued commitment to protecting the EY organization and client data is demonstrated through EY disaster recovery and business continuity capabilities. EY is 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 critical EY services applications have been carefully planned and tested. EY disaster recovery and business continuity methodologies incorporate the following:

- Business impact assessments
- Mission-critical disaster recovery plans built on industry-leading 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 EY 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 EY 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

EY teams 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
The EY 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 EY personal and client information assets. EY teams 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.

EY people are proactive in helping secure and properly manage confidential and personal information through the EY ISO 27001/2 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. EY teams maintain an effective governance function and reviews compliance through formal audit exercises. EY people also help manage 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 the EY security certification process to confirm that they have been developed in accordance with EY 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 behalf of EY professionals. This process helps EY teams maintain the confidentiality, integrity and availability of EY information and that of EY clients.

Privacy and confidentiality impact assessments
EY teams conduct privacy and confidentiality impact assessments of applications and business initiatives that handle personal or client information. Each privacy impact assessment (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 analysis includes a review of any cross-border data transfers to confirm these meet EU requirements.

EY organizations have a broad suite of policies and guidelines that helps in deployment of applications in accordance with applicable data protection standards and requirements.

Control effectiveness assessments
To verify that controls are implemented and operating effectively, EY teams perform several assessments of control effectiveness, including:

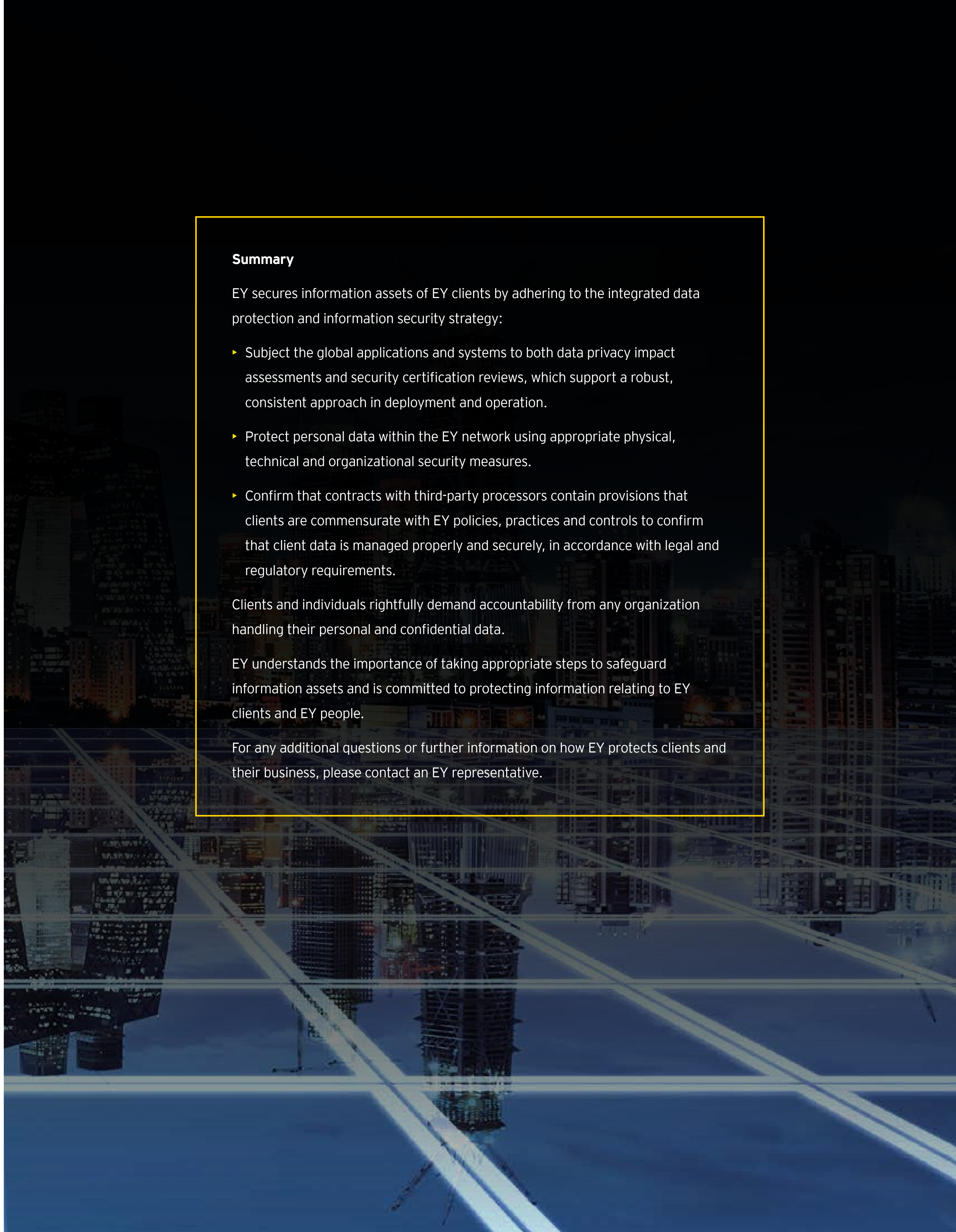
- Network and application vulnerability assessments, which focus on the technical aspects of the Global Information Security Policy, such as patch management, application security and infrastructure security
- Operating effectiveness assessments, which review technical controls and build processes of 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 the firm's three global data centers in the US, Germany and Singapore and local data rooms
- Annual SOC 2, Type 2 attestation conducted by an independent third-party auditor, which encompasses the security, confidentiality and availability principles and covers the firm's three global data centers in the US, Germany and Singapore and the third-party cloud-based EY Fabric, the client technology platform
- Annual ISAE 3402/SOC 1, Type 2 attestation of the organization's three global data centers in the US, Germany and Singapore and the third-party cloud-based EY Fabric, through which EY security controls are tested and verified by an independent third-party auditor
- Network vulnerability scans that focus on the technical aspects of 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 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 revisited at a future date.



Summary

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

- Subject the global applications and systems to both data privacy impact assessments and security certification reviews, which support a robust, consistent approach in deployment and operation.
- Protect personal data within the EY network using appropriate physical, technical and organizational security measures.
- Confirm that contracts with third-party processors contain provisions that clients are commensurate with EY policies, practices and controls to 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.

EY understands the importance of taking appropriate steps to safeguard information assets and is 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.

EYG no. 010715-22Gbl

2207-4070931 | ED None

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

ey.com