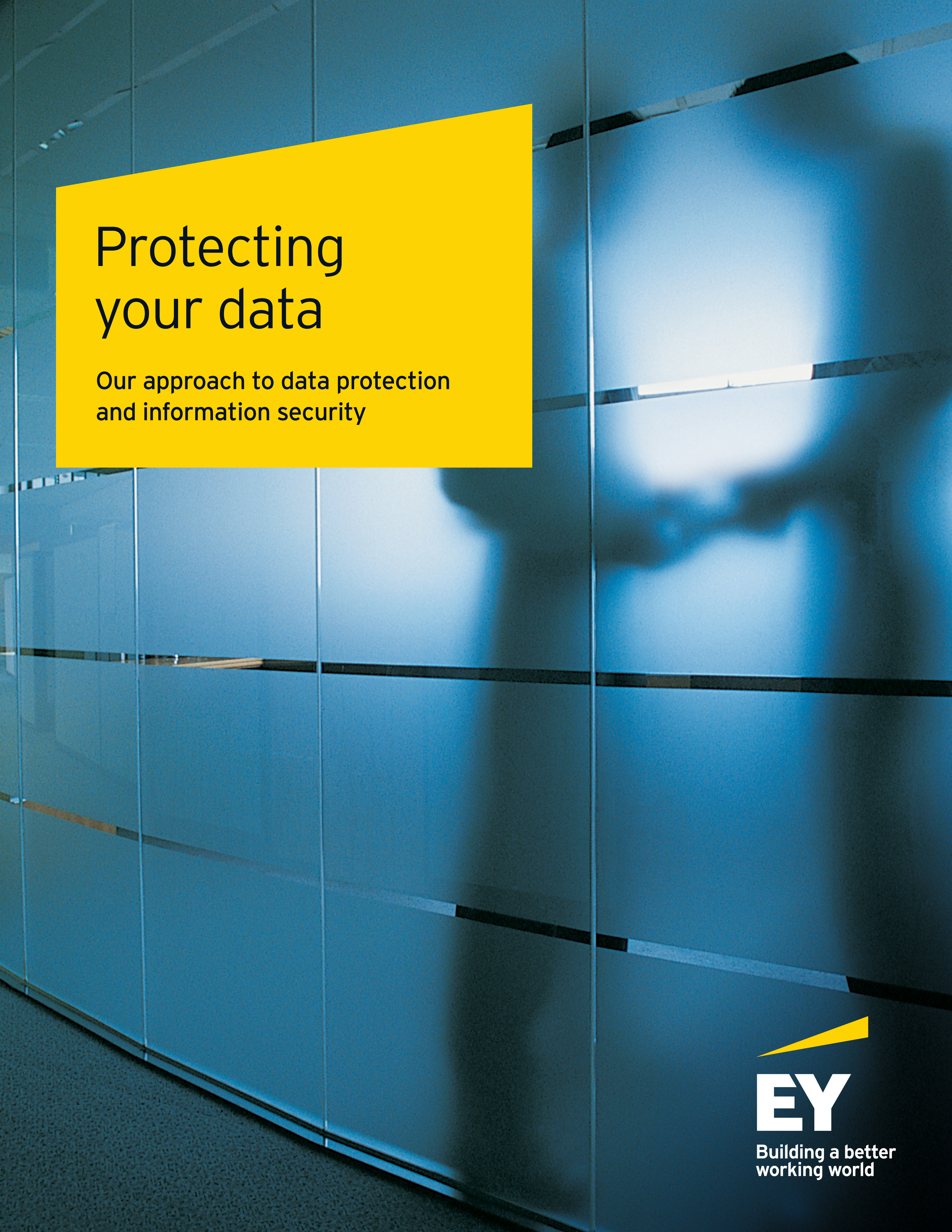
Protecting your data

Our approach to data protection and information security



EY

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 the essential components of a leading professional services organization. The purpose of this document is to summarize our approach to data protection and information security. It provides 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 security and data protection strategy

The EY team's ability to provide seamless, consistent, high-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 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 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, 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 our information assets, personal data and client information.

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

- We protect personal data using appropriate physical, technical and organizational security measures. These security measures are designed to facilitate compliance with data protection requirements by design and by default.
- 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 in accordance with the same standards we implement across the enterprise.
- We give additional attention and care to sensitive personal data.
- We have identified appropriate measures to keep personal data accurate, complete, current, adequate and reliable.
- We only retain personal data in a form that permits identification for as long as necessary.
- 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 data.
- We 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 our data protection framework

International data transfers
The international transfer of personal data is strictly regulated by European data protection law. Countries outside the European Economic Area without a comprehensive legislative approach to data protection are not deemed by the EU to provide an adequate level of protection for individuals' data privacy rights. Data protection law in Europe therefore prohibits the transfer of personal data to these countries unless the organization transferring the information has implemented appropriate legal safeguards.

Our teams have established 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 us to transfer personal data seamlessly within EY member firms, facilitating cross-service-line teaming. Although the legal obligations under European law apply only to personal data used and collected in the EU, we have applied these BCRs across the globe. Our BCRs are published at ey.com/bcr.

Our teams also make use of EU-approved Standard Contractual Clauses in contracts with clients and third parties where appropriate.

In addition, the EY member firm in the US is certified to the EU-US and Swiss-US Privacy Shield Frameworks. The Court of Justice of the European Union (CJEU) has invalidated the EU-US Privacy Shield framework as a mechanism for transferring personal data from the EEA to the US. Additionally, the Swiss Federal Data Protection and Information Commissioner has concluded in a paper that the Swiss-US Privacy Shield no longer provides an adequate level of protection for the transfer of personal data from Switzerland to the US. Nonetheless, the US member firm is committed to complying with the principles of the Privacy Shield framework even though it does not rely upon them to legitimize personal data transfers.

Alignment of our global data protection and information security priorities supports a single, cohesive vision concerning the protection of our 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, and it is reflected not only in mandatory training updated regularly for professionals in each of EY service lines, but 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 by senior management to confirm that the material remains timely and accurate, and that it correlates to legal and regulatory requirements applicable to us. Mandatory and recommended policy statements span nearly a dozen widely recognized information security areas, including, but not limited to:

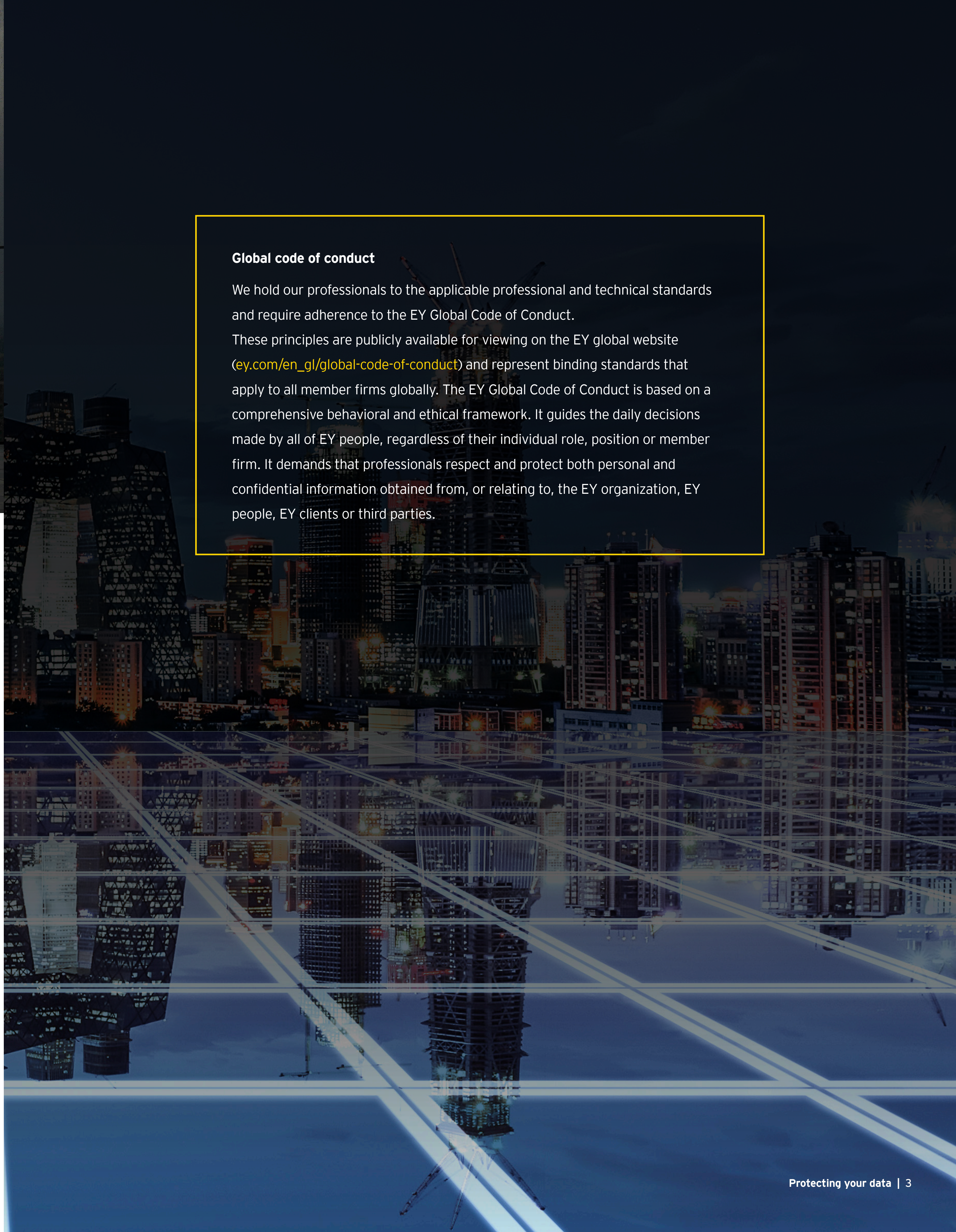
- Access control
- Asset management: classification and control
- Communications and operations security
- Human resources security: personnel
- Information systems acquisition, development and maintenance
- Physical and environmental security
- Risk assessment

Technical security controls
Our approach to information security does not rely solely upon a 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:

- 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 road map 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.

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



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 principles are publicly available for viewing on the EY global website (ey.com/en_gl/global-code-of-conduct) and represent binding standards 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 of EY people, regardless of their individual role, position or member firm. It demands 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
Our continued commitment to protecting organization and client data is demonstrated through our disaster recovery and business continuity capabilities. 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-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
Our supplier risk assurance 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
- 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 our global information security and personal conduct policies. 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 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 road map 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

Our teams have global data protection and information security programs. We maintain an effective governance function, and we conduct compliance reviews through formal audit exercises. We 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 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
We conduct privacy and confidentiality impact assessments (PIAs) of applications and business initiatives that handle personal or client 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 includes a review of any cross-border data transfers to confirm these meet EU requirements.

Our organizations have a broad suite of policies and guidelines that helps us deploy applications 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 us with 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:

- Independent third-party compliance audits against ISO 27001:2013 to certify the Information Security Management System employed within our 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 our three global data centers in the US, Germany and Singapore and the third-party cloud-based EY Client Technology Platform
- Annual ISAE 3402/SOC 1, Type 2 attestation of our three global data centers in the US, Germany and Singapore and the third-party cloud-based EY Client Technology Platform, through which our security controls are tested and verified by an independent third-party auditor
- Network vulnerability scans, which focus on the technical aspects of our 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 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 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

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

- We 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.
- We protect personal data within our network using appropriate physical, technical and organizational security measures.
- We confirm that our contracts with third-party processors contain provisions that are commensurate with our own policies, practices and controls to confirm that 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 EY clients and EY 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 | 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. 000907-21Gbl
CSG no. 2011-3646208

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