Data Protection Guidelines for Suppliers

Latam

2025

The better the question.
The better the answer.
The better the world works.

Shape the future with confidence

At EY, the protection of Confidential Information and Personal Data is a fundamental legal and professional obligation. As part of our commitment to maintaining the highest standards of privacy, confidentiality, and regulatory compliance, we expect all our suppliers ("Suppliers") to uphold these principles when delivering services on our behalf or even when providing services to us. Personal Data and Confidential Information – whether belonging to EY or its clients – are critical assets, and their responsible handling is essential to preserving trust and meeting the Applicable Laws, even data protection requirements.

This document outlines EY's expectations and provides practical guidance for Suppliers delivering professional services to EY. **It is designed to ensure that Personal Data and Confidential Information are safeguarded throughout the entire service lifecycle, in alignment with EY's internal policies and Applicable Laws.** Suppliers are required to comply with EY's policies and procedures and to adhere to these guidelines as part of their contractual and ethical responsibilities when working with EY.

For the purposes of this document, the term "Data" will be used broadly to refer to both Personal Data and other types of Confidential Information - such as third-party information, client information and EY business information-, including but not limited to sensitive, confidential, or proprietary data, as defined by Applicable Laws and internal EY policies, procedures and standards.

Please note that this document provides only the general principles and minimal guidelines that the Suppliers must comply with. Each Latam's EY Member Firm is responsible for the compliance and the engagement of its Suppliers and can have or apply more restrictive provisions.

Sumary

General Principles for Data Handling

All Suppliers providing services to EY must adhere to the following core principles, which reflect EY's commitment to responsible data stewardship and compliance with Applicable Laws. These principles apply throughout the entire Data lifecycle and must guide all Data processing activities:

1 Lawfulness, Fairness, and Transparency

Data must be processed in a lawful, fair, and transparent manner. Suppliers must ensure that individuals are informed – directly by the re-Supplier, through EY or as instructed – about how their Data is being used and must not process Data in ways that are misleading or outside the agreed purpose.

2 Purpose Limitation

Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Suppliers must only use the Data for the purposes defined in their agreement with EY.

3 Data Minimization

Only the minimum amount of Data necessary for the intended purpose should be collected and processed. Suppliers must avoid collecting or keeping excessive or irrelevant Data.

4 Accuracy

Data must be accurate and, where necessary, kept up to date. Suppliers are responsible for implementing processes to correct or delete inaccurate Data without delay.

5 Storage Limitation

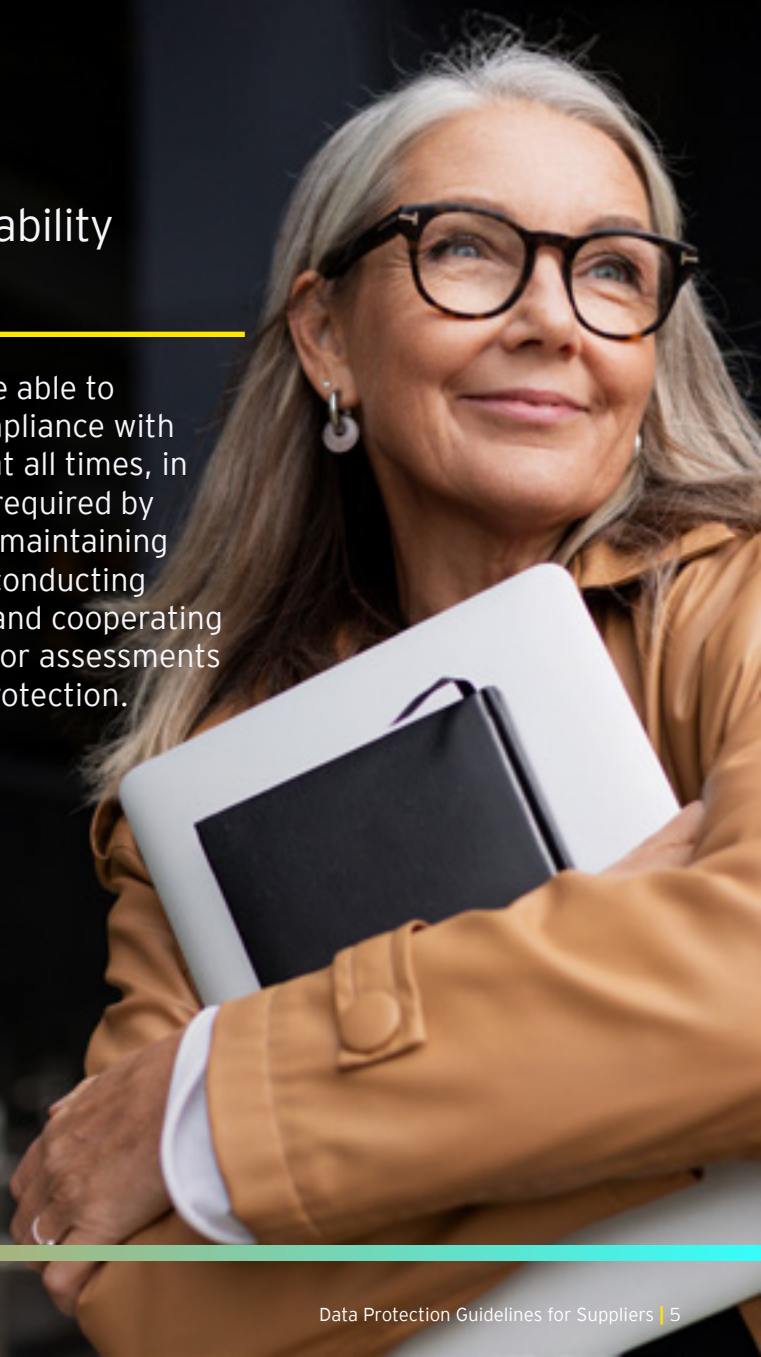
Data must not be kept for longer than necessary and in accordance with the Applicable Laws. Suppliers must follow EY's retention instructions and securely return and delete Data once the purpose has been fulfilled or the services are concluded unless the Applicable Laws require the retention of the Data for a specific term.

6 Integrity and Confidentiality (Security)

Data must be processed in a manner that ensures appropriate security, including protection against Data Incident, including, but not limited to unauthorized or unlawful processing, accidental loss, destruction, or damage. Suppliers must implement robust technical and organizational security measures.

7 Accountability

Suppliers must be able to demonstrate compliance with these principles at all times, in particular, when required by EY. This includes maintaining documentation, conducting regular reviews, and cooperating with EY in audits or assessments related to data protection.



Protecting Data Throughout the Service Lifecycle

To ensure the responsible handling of Data throughout the provision of services to EY, Suppliers are required to follow specific recommendations. These recommendations (or guidelines) are structured across three key phases of the service lifecycle:

1

Service Initiation

At the outset of any service, Suppliers must take proactive steps to establish a secure and compliant Data environment:

1

Data Classification
Understand the nature and sensitivity of the Data to be handled, including its classification (e.g., confidential, personal, sensitive, public).

Data Minimization
Identify and collect only the Data strictly necessary for the delivery of services.

Purpose Definition
Clearly define the purpose for which Data will be processed, ensuring alignment with EY's instructions and contractual terms.

Access Controls
Implement role-based access to Data, limiting exposure to authorized personnel only.

Data Processing Agreements ("DPA")
Ensure that all relevant Data protection clauses or a specific DPA are included in the relevant agreements and that contractors or subcontractors, if any, are bound by equivalent obligations.

Security Planning:
Establish appropriate technical and organizational measures to protect Data from any Data Incident.

Transmission Methods:
Assess and apply secure transmission methods (e.g., encrypted email, secure file transfer protocols, EY´s transmission tools) appropriate to the Data type and risk level.

Consultation and Clarification:
Engage with your designated EY contact to clarify any uncertainties regarding Data handling requirements, transmission protocols, or compliance expectations. Open communication at this stage is essential to ensure alignment and prevent mismanagement of Data.

2

During the Service

Throughout the service delivery, Suppliers must maintain robust Data protection practices and monitor compliance:

2

Secure Processing
Suppliers must apply security and data protection measures defined during the initial phase of the service. All Data must be processed in accordance with the transmission methods, access controls, and security protocols previously agreed upon with EY. Any deviation from these standards must be approved by your designated EY contact. EY shall not be held liable for any such deviations or for any non-compliance with Applicable Law resulting from the Supplier's actions.

Monitoring and Auditing
Conduct periodic internal reviews to verify that Data handling practices remain compliant with EY's requirements and Applicable Laws. Findings should be documented and corrective actions taken promptly.

Data Access Monitoring
Continuously monitor who has access to Data and ensure that access is limited to individuals with a legitimate business need. Any changes in personnel or roles must be reflected in access permissions immediately.

Incident Management
Maintain a documented process for identifying, reporting, and responding to Data Incidents. In some instances, EY must be notified immediately about Data Incidents in accordance with contractual and legal obligations.

Training and Awareness
Ensure that all personnel (e.g., Suppliers employees, legal representatives and contractors) involved in Data processing are trained on data protection principles and EY's specific requirements.

Service Conclusion

At the end of the services, Suppliers must ensure that Data is properly handled to prevent residual risks:

- **Data Return or Deletion:** Upon completion of the service, Suppliers must return all Data to EY in accordance with contractual obligations and EY's instructions. If no return is required, or once the return has been completed, Suppliers must proceed with the secure deletion of all Data from their systems.

- **Access Revocation and Data Cleanup:** Remove any unnecessary access rights to any systems, platforms, or data repositories. Ensure that all residual Data stored locally or in cloud environments is securely deleted and cannot be recovered.

- **Formal Confirmation:** Provide EY with formal confirmation of Data deletion or return. This may include secure destruction certificates, signed records, or other verifiable documentation that demonstrates compliance with EY's data handling requirements.

- **Post-Service Review:** Conduct a final review to ensure no Data remains in Supplier systems or backups.

- **Retention Policies:** Ensure that no Data is retained beyond the agreed retention period unless legally required.

- **No Data Reuse:** Data obtained during the engagement must not be reused for any other purpose or project unless explicit written consent has been obtained from EY. Unauthorized reuse constitutes a breach of contractual and legal obligations.

3

Additional Guidelines on Data Security and Protection

The following recommendations are intended to reinforce data security practices across all stages of service delivery. Suppliers must adhere to these guidelines in addition to the general principles and lifecycle recommendations outlined in this document.

Data Subject Requests

- Immediately notify your designated EY contact upon receiving any request from a Data Subject (e.g., access, rectification, deletion) unless the Supplier is responsible for the processing and the compliance with this obligation (i.e., the Supplier acts as an independent data controller according to the Applicable Law).

- Do not respond or share any Data without explicit written authorization from EY unless legally required.

- Be prepared to support EY in fulfilling Data Subject rights in a timely and compliant manner.

Data Incidents

- Report any confirmed or suspected Data Incidents, breaches, or security vulnerabilities to your designated EY contact immediately.

- Do not disclose Data Incident details to third parties unless explicitly authorized by EY unless legally required.

- Follow EY's Data Incident response protocols and cooperate fully in investigations and remediation efforts.

- In some jurisdictions, the communication of a Data Incident is required for the relevant Data Subjects and even the Data Protection Supervisory Authorities, the Applicable Law requirements must be followed.

Use of Technological Tools

- The use of technology must align with applicable laws, regulations, and EY's requirements.

- Technology, including artificial intelligence, should be used to support – not substitute – the supplier's professional expertise, responsibilities, and ethical standards when delivering services to EY.

- Suppliers are expected to stay informed about the risks, limitations, and evolving capabilities of emerging technologies to ensure responsible and effective use.

- When transmitting Sensitive Personal Data, Suppliers must apply enhanced protection measures (e.g., encrypted email, secure file transfer protocols, EY´s transmission tools).

Data Security Practices

- Always verify email recipients and attachments before sending messages containing Data.
- Avoid forwarding Data to personal email accounts or unauthorized recipients.
- Maintain physical security of portable devices (e.g., laptops, USB drives); avoid leaving them powered on or unattended.
- Prevent unauthorized access to work devices by locking screens and using strong passwords.
- Avoid discussing confidential matters in public or unsecured environments.
- When working remotely, ensure the workspace is private and secure, and use approved tools and secure networks.
- Avoid printing or transporting physical documents unless strictly necessary and protect physical documents from unauthorized access, especially when working off-site.
- Apply strong passwords and multi-factor authentication ("MFA") to your systems and do not share system credentials or access tokens with others.

Networks and Access Control

- Validate the legitimacy of public Wi-Fi networks before connecting; prefer password-protected networks and use VPNs when available.

- Apply the “need-to-know” principle when sharing Data, limiting access to only those who require it for service delivery.

- Conduct periodic reviews of access permissions to collaborative platforms and Data repositories.

Definitions

Applicable law: Any laws, rules, regulations or directives, including but not limited to privacy and data protection matters, applicable to the Supplier.

Data: This term is used broadly to refer to both Personal Data and other types of Confidential Information - such as third-party information, client information and EY business information-, including but not limited to sensitive, confidential, or proprietary data, as defined by Applicable Laws and internal EY policies, procedures and standards.

Data Subject: The individual to whom the collected information relates, as defined under Applicable Law.

Confidential Information: Any information related to EY and its clients is processed according to an engagement with EY. Client Information means any information relating to the affairs of a current or former client obtained by EY from a client or from a third party in connection with an engagement with such a client. On the other hand, EY information means (i) Personal Data; (ii) third party information; (iii) client information; and (iv) EY business information.

Data Incident: Any event that compromises the security, confidentiality, integrity or availability of any Data, including any unauthorized or inappropriate disclosure, loss, use, destruction, alteration of, or access to Data.

Personal Data: Means (i) any information that alone or together with any other information relates to an identified or identifiable natural person (such as name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person), and (ii) any other information considered to be personally identifiable information, personal data or personal information (or similar term) under applicable law.

Sensitive Personal Data: Refers to Personal Data that, according to applicable law, is considered sensitive due to its potential to affect the Data Subject's privacy or lead to discrimination. This includes, but is not limited to, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data used for identification purposes, health-related data, and data concerning a natural person's sex life or sexual orientation. Additionally, Personal Data related to criminal convictions and offenses, as well as data that may facilitate identity theft or payment fraud (such as financial account numbers, credit card details, and government-issued identification numbers), are considered sensitive, to the extent defined by the applicable law.

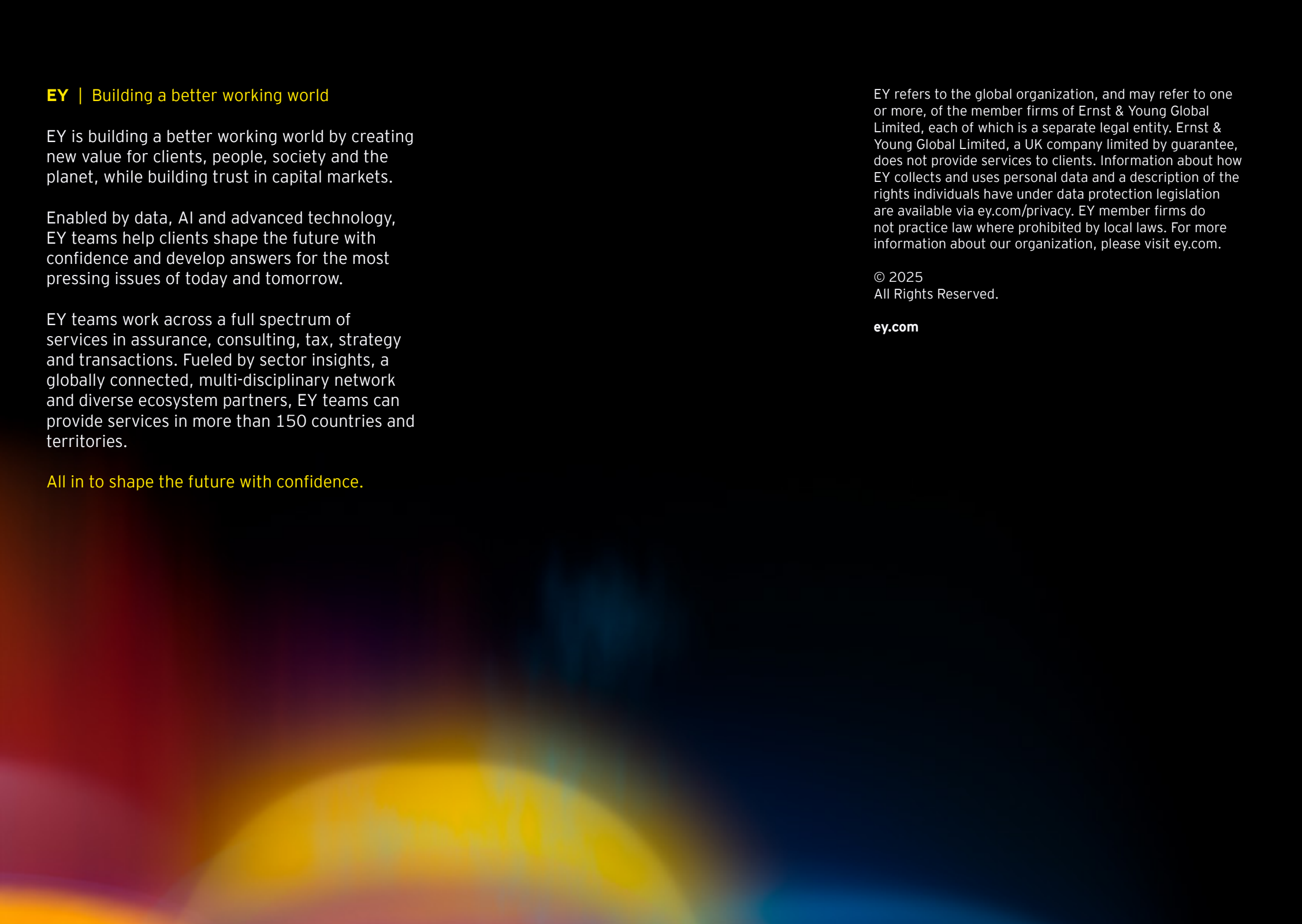
EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.



ey.com