Lineamientos de Protección de Datos para Proveedores

Latam

2025

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

Shape the future with confidence

En EY, la protección de Información Confidencial y Datos Personales es una obligación legal y profesional fundamental. Como parte de nuestro compromiso de mantener los estándares más altos de privacidad, confidencialidad y cumplimiento normativo, esperamos que todos nuestros proveedores ("Proveedores") mantengan estos principios al prestar servicios en nuestro nombre o incluso al brindarnos servicios directamente. La Información Confidencial y Datos Personales — ya sea que pertenezcan a EY o a sus clientes — son activos críticos, y su gestión responsable es esencial para preservar la confianza y cumplir con las Leyes Aplicables, incluyendo los requerimientos en materia de protección de Datos.

Este documento establece las expectativas de EY y proporciona una orientación práctica para los Proveedores que presten servicios profesionales a EY. **Está diseñado para garantizar que los Datos Personales e Información Confidencial sean protegidos durante la prestación del servicio, de conformidad con las políticas internas de EY y las Leyes Aplicables.** Se requiere que los Proveedores cumplan con las políticas y procedimientos de EY, y que se adhieran a estas directrices como parte de sus responsabilidades contractuales y éticas al trabajar con EY.

A efectos de este documento, el término "Datos" será utilizado de manera amplia para referirse a los Datos Personales y otros tipos de Información Confidencial – como la información de terceros, información de clientes e información empresarial de EY –, incluyendo, pero sin limitarse a los Datos Personales Sensibles, confidenciales o propietarios, tal como es definido en las Leyes Aplicables y las políticas, procedimientos, y estándares internos de EY.

Tenga en cuenta que este documento proporciona únicamente los principios generales y lineamientos mínimos que los Proveedores deben cumplir. Cada Firma Miembro de EY en Latinoamérica es responsable del cumplimiento y compromiso de sus Proveedores, y pueden incluir o establecer medidas más restrictivas.

Sumary

Principios Generales del Manejo de Datos

Todos los Proveedores que presten servicios a EY deben adherirse a los siguientes principios fundamentales, los cuales reflejan el compromiso de EY con la administración responsable de Datos y el cumplimiento de las Leyes Aplicables. Estos principios son aplicables a todo el ciclo de vida de los Datos y deben orientar todas las actividades en donde estos se procesen:

1 Legalidad, Justicia y Transparencia

Los Datos deben ser procesados de manera legal, justa y transparente. Los Proveedores deben garantizar que los individuos estén informados — directamente por el Proveedor, a través de EY o conforme a lo indicado — sobre cómo sus Datos están siendo utilizados y no deben procesar Datos de forma engañosa o en contravención de la finalidad convenida.

2 Limitación de la Finalidad

Los Datos deben ser recopilados para fines específicos, explícitos y legítimos, y no serán procesados posteriormente de una manera incompatible con estos fines. Los Proveedores solo deben utilizar los Datos para la finalidad determinada en lo acordado con EY.

3 Minimización de Datos

Solo se debe recopilar y procesar la cantidad mínima de Datos necesarios para la finalidad pretendida. Los Proveedores deben evitar recolectar o mantener Datos excesivos o irrelevantes.

4 Precisión

Los Datos deben ser precisos y, cuando sea necesario, actualizados. Los Proveedores son responsables por la implementación de procesos para corregir o eliminar la información imprecisa con prontitud.

5 Limitación de Almacenamiento

Los Datos no deben conservarse por más tiempo del necesario y de conformidad con las Leyes Aplicables. Los Proveedores deben seguir las instrucciones de retención de EY y devolver o eliminar de forma segura los Datos una vez cumplida su finalidad o culminado el servicio, salvo que las Leyes Aplicables exijan la conservación de los Datos por un término específico.

6 Integridad y Confidencialidad (Seguridad):

Los Datos deben ser procesados de tal manera que se garantice su seguridad apropiada, protegiéndolos contra Incidentes de Datos, tales como el tratamiento no autorizado o ilícito, la pérdida accidental, destrucción o daño. Los Proveedores deben implementar medidas de seguridad técnicas y organizativas robustas.

7 Responsabilidad

Los Proveedores deben ser capaces de demostrar el cumplimiento de estos principios en todo momento, en particular cuando así lo requiera EY. Esto incluye mantener la documentación correspondiente, realizar revisiones periódicas y cooperar con EY en auditorías o evaluaciones relacionadas con la protección de Datos.

Protección de Datos Durante Todo el Ciclo de Vida de la Prestación del Servicio

1

Para garantizar el manejo responsable de los Datos durante la provisión de servicios a EY, los Proveedores están obligados seguir recomendaciones específicas. Estas recomendaciones (o lineamientos) están estructuradas a lo largo de las 3 etapas del ciclo de vida del servicio:

Inicio del Servicio

1

Desde el inicio de cualquier servicio, los Proveedores deben tomar medidas proactivas para establecer un entorno seguro y en cumplimiento:

Clasificación de Datos: Comprender la naturaleza y sensibilidad de los Datos que se deben manejar, incluyendo su clasificación (por ejemplo, confidencial, personal, sensible, público).

Minimización de Datos: Identificar y recolectar solo los Datos estrictamente necesarios para la prestación de servicios.

Definición de la Finalidad: Definir claramente el propósito para el cual se procesarán los Datos, asegurando que sea conforme a las instrucciones y términos contractuales establecidas por EY.

Control de Acceso: Implementar controles de acceso a los Datos basado en roles, limitando su exposición únicamente al personal autorizado.

Acuerdo de Procesamiento de Datos (DPA, por sus siglas en inglés): Asegurarse de que todas las cláusulas relevantes de protección de Datos, o un Acuerdo de Protección de Datos específico, estén incluidas en los contratos correspondientes, y que los contratistas o subcontratistas, en caso de haberlos, estén sujetos a obligaciones equivalentes.

Planificación de Seguridad: Establecer las medidas técnicas y organizativas adecuadas para proteger los Datos frente a cualquier Incidente de Datos.

Métodos de Transmisión: Evaluar y aplicar métodos seguros de transmisión (por ejemplo, correo electrónico cifrado, protocolos seguros de transferencia de archivos o herramientas de transmisión de EY), adecuados al tipo de Datos y al nivel de riesgo asociado.

Consulta y Aclaración: Comuníquese con su contacto designado de EY para aclarar cualquier duda relacionada al manejo de Datos, protocolos de transmisión, o expectativas de cumplimiento. La comunicación abierta en esta etapa es esencial para asegurar la alineación y prevenir una gestión inadecuada de los Datos.

2

Durante el Servicio

Durante la prestación del servicio, los Proveedores deben mantener una práctica de protección de Datos robusta y monitorear su cumplimiento:

2

Procesamiento Seguro
Los Proveedores deben aplicar las medidas de seguridad y protección de Datos definidas durante la fase inicial del servicio. Todos los Datos deben ser tratados conforme a los métodos de transmisión, controles de acceso y protocolos de seguridad previamente acordados con EY. Cualquier desviación de estos estándares deberá contar con la aprobación de su contacto designado de EY. EY no será responsable por dichas desviaciones ni por cualquier incumplimiento de la Ley Aplicable que resulte de las acciones del Proveedor.

Monitoreo y Auditoría
Realizar revisiones internas periódicas para verificar que las prácticas de manejo de Datos continúan cumpliendo con los requisitos de EY y con la Ley Aplicable. Los hallazgos deben ser documentados y las acciones correctivas deben implementarse de manera inmediata.

Monitoreo del Acceso a los Datos
Supervisar de forma continua quién tiene acceso a los Datos y asegurarse de que dicho acceso esté limitado únicamente a personas con una necesidad legítima de negocio. Cualquier cambio en el personal o en los roles debe reflejarse de inmediato en los permisos de acceso.

Manejo de Incidentes
Mantener un proceso documentado de identificación, reporte y respuesta a los Incidentes de Datos. EY deberá ser notificado inmediatamente sobre Incidentes de Datos, en concordancia a las obligaciones contractuales y legales.

Formación y concientización
Asegurarse de que todo el personal involucrado en el tratamiento de Datos (por ejemplo, empleados, representantes legales y contratistas del Proveedor) reciba capacitación sobre los principios de protección de Datos y los requisitos específicos de EY.

Conclusión del servicio

Al final del servicio, los Proveedores deben garantizar que los Datos son manejados adecuadamente para prevenir riesgos residuales:

▸ **Devolución o Eliminación de los Datos:** Al finalizar la prestación del servicio, los Proveedores deben devolver todos los Datos a EY en concordancia con las obligaciones contractuales e instrucción de EY. Si no se requiere devolver los Datos, o una vez se devuelvan los Datos, los Proveedores deben eliminar de manera segura los Datos en sus sistemas.

▸ **Revocación de Acceso y Eliminación de Datos:** Eliminar cualquier derecho de acceso innecesario a sistemas, plataformas o repositorios de Datos. Asegurar que todos los Datos residuales almacenados localmente o en entornos en la nube sean eliminados de forma segura y no puedan ser recuperados.

▸ **Confirmación Formal:** Proporcionar a EY una confirmación formal de la eliminación o devolución de Datos. Esto puede incluir certificados de destrucción, registros firmados, u otros documentos verificables que demuestren el cumplimiento de los requerimientos de manejo de Datos de EY.

▸ **Revisión Posterior a la Prestación del Servicio:** Realizar una revisión final para asegurarse de que no queden Datos en los sistemas o respaldos (copias de seguridad) del Proveedor.

▸ **Políticas de Retención:** Garantizar que no haya Datos retenidos o conservados más allá del período acordado, salvo que sea legalmente requerido.

▸ **No Reutilización de Datos:** Los Datos obtenidos durante la prestación del servicio no deben ser reutilizados para otros fines o proyectos, a menos que se cuente con el consentimiento explícito y por escrito de EY. La reutilización no autorizada constituye un incumplimiento de las obligaciones contractuales y legales.

3

Lineamientos Adicionales sobre Protección y Manejo de Datos

Las siguientes recomendaciones están destinadas a reforzar las prácticas de seguridad de Datos en todas las etapas de la prestación de servicios. Los Proveedores deben cumplir con estos lineamientos además de los principios generales y las recomendaciones sobre el ciclo de vida descritas en este documento.

Solicitud del Titular de los Datos

- Informar inmediatamente a su contacto designado de EY al recibir cualquier solicitud de un Titular de Datos (por ejemplo, acceso, rectificación, eliminación), a menos que el Proveedor sea responsable del tratamiento y del cumplimiento de esta obligación (es decir, que actúe como responsable independiente del tratamiento conforme a la Ley Aplicable).

- No responda ni comparta ningún Dato sin la autorización explícita y por escrito de EY, a menos que exista una obligación legal que lo requiera.

- Estar preparado para apoyar a EY en el cumplimiento de los derechos de los Titulares de Datos de manera oportuna y adecuada.

Data Incidents

- Informar de inmediato a su contacto designado de EY sobre cualquier Incidente de Datos confirmado o sospechoso, brecha de seguridad o vulnerabilidad.

- No divulgar los detalles de los Incidentes de Datos con terceros, salvo que sea explícitamente autorizado por EY o legalmente requerido.

- Seguir los protocolos de respuesta de EY sobre Incidentes de Datos, y coopera plenamente en investigaciones y esfuerzos de remediación.

- En algunas jurisdicciones, la comunicación de un Incidente de Datos es obligatoria tanto para los Titulares de Datos como para las Autoridades de Supervisión de Protección de Datos correspondientes; debiendo cumplir los requisitos establecidos por la legislación vigente.

Uso de Herramientas Tecnológicas

- El uso de herramientas tecnológicas debe ser conforme a las leyes aplicables, regulación, y requerimientos de EY.

- La tecnología, incluida la inteligencia artificial, debe utilizarse para apoyar y no reemplazará la experticia profesional, las responsabilidades y los estándares éticos del Proveedor al prestar servicios a EY.

- Se espera que los Proveedores se mantengan informados sobre los riesgos, limitaciones, y capacidades en evolución de las tecnologías emergentes, con el fin de asegurar su uso responsable y efectivo.

- Al transmitir Datos Personales Sensibles, los Proveedores deben aplicar medidas de protección reforzadas (por ejemplo, correos electrónicos encriptados, protocolos de transferencia segura de Datos, herramientas de transmisión de EY).

Prácticas de Seguridad de Datos

- Verificar siempre los destinatarios del correo electrónico y los archivos adjuntos antes de enviar mensajes que contengan Datos.

- Evitar el reenvío de Datos a cuentas de correos electrónicos personales o destinatarios no autorizados.

- Mantener la seguridad física de los dispositivos portátiles (por ejemplo, laptops, unidades USB); evite dejarlos encendidos o sin supervisión.

- Prevenir el acceso no autorizado a los dispositivos corporativos mediante el bloqueo de pantallas y el uso de contraseñas seguras.

- Evitar discutir sobre asuntos confidenciales en público o entornos no seguros.

- Al trabajar de manera remota, garantizar que el espacio de trabajo sea privado y seguro, utilizando herramientas aprobadas y redes seguras.

- Evitar imprimir o transportar documentos físicos, salvo que sea estrictamente necesario, y proteger documentos físicos de accesos no autorizados, especialmente al trabajar fuera de las instalaciones.

- Aplicar a sus sistemas contraseñas seguras y autenticación multifactorial (MFA, por sus siglas en inglés), y no compartir credenciales del sistema o token de acceso con otras personas.

Redes y Control de Acceso

- Validar la legitimidad de redes públicas de Wi-Fi antes de conectarte; preferir aquellas protegidas con contraseña y utilice VPNs cuando estén disponibles.

- Aplique el principio de “necesidad de saber” al compartir Datos, limitando el acceso únicamente a quienes lo requieran para la prestación del servicio.

- Dirigir revisiones periódicas de permisos de acceso de plataformas colaborativas y repositorios de Datos.

Definiciones

Ley Aplicable: Cualquier ley, regla, regulación o directiva, incluyendo, pero no limitándose a los asuntos de privacidad y protección de Datos aplicables para el Proveedor.

Datos: Este término es utilizado de manera amplia al referirse a Datos Personales y otros tipos de Información Confidencial — como la información de terceros, información de clientes e información corporativa de EY —, incluyendo, pero no limitándose, a Datos Personales Sensibles, confidenciales o propietarios, según lo definido por las Leyes Aplicables y las políticas, procedimiento y estándares internos de EY.

Titular de los Datos: El individuo al que se refiere la información recopilada, según lo definido por la Ley Aplicable.

Información Confidencial: Cualquier información relacionada a EY y sus clientes será procesada de conformidad con lo acordado con EY. La información del cliente se refiere a cualquier información relacionada con los asuntos de un cliente actual o anterior, obtenida por EY de un cliente o tercero relacionado al acuerdo con dicho cliente.
Por otro lado, la información de EY significa i) Datos Personales, ii) información de terceros; iii) información de clientes; iv) información corporativa de EY.

Incidentes de Datos: Cualquier evento que comprometa la seguridad, confidencialidad, integridad o disponibilidad de cualquier Dato, incluyendo cualquier divulgación no autorizada o inapropiada, pérdida, uso, destrucción, alteración, o acceso a los Datos.

Datos Personales: Significa i) cualquier información que por sí sola o en conjunto con cualquier otra, se refiera a una persona natural o individuo que pueda ser identificado o identificable (como nombre, número de identificación, datos de ubicación, identificadores en línea, o uno o más factores específicos sobre identidad física, fisiológica, mental, económica, cultural o social de esa persona natural o individuo), y ii) cualquier información considerada como información personal identificable, datos personales o información personal (u otro término similar) bajo la Ley Aplicable.

Datos Personales Sensibles: Se refiere a los Datos Personales que, de acuerdo con la Ley Aplicable, son considerados sensibles debido a su potencial efecto en la privacidad del Titular de los Datos o lleve a discriminación. Esto incluye, pero no se limita, a revelar datos raciales o de origen étnico, opiniones políticas, religiosas o creencias filosóficas, afiliación sindical, datos genéticos, datos biométricos utilizados para fines de identificación, datos relacionados con la salud, y datos relativos a la vida u orientación sexual de una persona natural o individuo. Adicionalmente, los Datos Personales relacionados a condenas penales y delitos, así como los datos que faciliten la suplantación de identidad o fraude en medios de pago (como números de cuentas financieras, detalles de tarjetas de crédito, y números de identificación emitidos por el gobierno), son considerados como datos sensibles, en la medida que lo defina la Ley Aplicable.

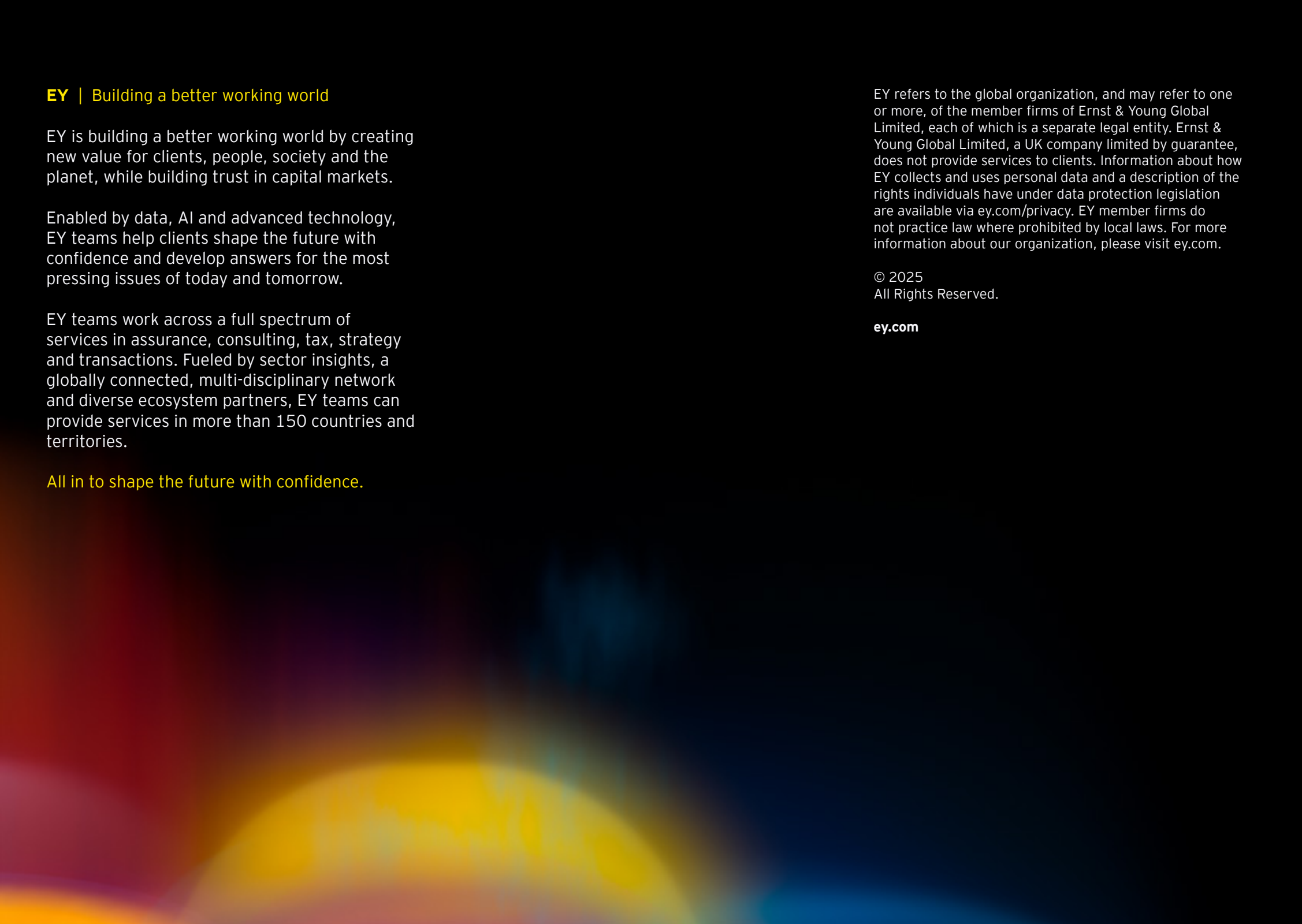
EY | Building a better working world

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