Diretrizes de Proteção de Dados para Fornecedores e Prestadores de Serviços Latam

2025

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

EY

Shape the future with confidence

Na EY, a proteção de Informações Confidenciais e Dados Pessoais é uma obrigação legal e profissional fundamental. Como parte do nosso compromisso em manter os mais altos padrões de privacidade, confidencialidade e conformidade regulatória, esperamos que todos os nossos fornecedores e prestadores de serviços ("Fornecedores") mantenham esses princípios ao fornecer serviços em nosso nome ou mesmo ao fornecer serviços para nós. Dados Pessoais e Informações Confidenciais – sejam pertencentes ou de responsabilidade primária da EY ou de seus clientes – são ativos críticos, e seu manuseio responsável é essencial para preservar a confiança e cumprir as Leis Aplicáveis.

Este documento (“Diretrizes”) descreve as expectativas da EY e fornece orientações práticas para os Fornecedores que prestam serviços profissionais à EY no que tange à proteção de dados e informações confidenciais. **Ele foi elaborado para garantir que os Dados Pessoais sejam protegidos durante todo o ciclo de vida do serviço prestado, em conformidade com as políticas internas da EY e as Leis Aplicáveis.** Os Fornecedores são obrigados a cumprir as políticas e procedimentos da EY e a aderir a estas Diretrizes como parte de suas responsabilidades contratuais e éticas ao trabalhar com a EY.

Para os fins deste documento, o termo “Dados” será usado de forma ampla para se referir tanto a Dados Pessoais quanto a Informações Confidenciais - como informações de terceiros, informações de clientes e informações comerciais da EY -, conforme definido pelas Leis Aplicáveis e pelas políticas, procedimentos e padrões internos da EY.

Observe que este documento fornece apenas os princípios gerais e as diretrizes mínimas que os Fornecedores devem cumprir. Cada Firma Membro da EY na região Latam é responsável pela conformidade e pelo engajamento de seus Fornecedores e pode ter ou aplicar disposições mais restritivas, conforme a necessidade.

Sumary

Princípios Gerais para o Tratamento de Dados

Todos os Fornecedores que prestam serviços à EY devem aderir aos seguintes princípios fundamentais, que refletem o compromisso da EY com a gestão responsável de Dados e a conformidade com as Leis Aplicáveis. Esses princípios se aplicam durante todo o ciclo de vida dos Dados e devem orientar todas as atividades de tratamento de Dados:

1 Licitude, Justiça e Transparência

Os Dados devem ser tratados de maneira lícita, justa e transparente. Os Fornecedores devem garantir que os indivíduos sejam informados — diretamente pelo Fornecedor, através da EY ou conforme instruído — sobre como seus Dados estão sendo usados e não devem tratar Dados de maneiras enganosas ou fora do propósito acordado.

2 Limitação de Propósito

Os Dados devem ser coletados para fins específicos, explícitos e legítimos e não devem ser tratados posteriormente de maneira incompatível com esses fins. Os Fornecedores devem usar os Dados apenas para os fins definidos em seu contrato firmado com a EY.

3 Minimização de Dados

Apenas a quantidade mínima de Dados necessária para o propósito pretendido deve ser coletada e tratada. Os Fornecedores devem evitar coletar ou manter Dados excessivos ou irrelevantes.

4 Precisão

Os Dados devem ser precisos e, quando necessário, mantidos atualizados. Os Fornecedores são responsáveis por implementar processos para corrigir ou excluir Dados imprecisos sem demora.

5 Limitação de Armazenamento

Os Dados não devem ser mantidos por mais tempo do que o necessário e de acordo com as Leis Aplicáveis. Os Fornecedores devem seguir as instruções de retenção da EY e devolver (se físicos, por exemplo) e excluir os Dados de forma segura uma vez que o propósito tenha sido cumprido ou os serviços concluídos, a menos que as Leis Aplicáveis exijam a retenção dos Dados por um período específico.

6 Integridade e Confidencialidade (Segurança)

Os Dados devem ser tratados de maneira que garanta segurança adequada, incluindo proteção contra Incidentes de Dados, incluindo, mas não se limitando a tratamento não autorizado ou ilegal, perda acidental, destruição ou danos. Os Fornecedores devem implementar medidas de segurança técnicas e organizacionais robustas.

7 Responsabilidade

Os Fornecedores devem ser capazes de demonstrar conformidade com esses princípios em todos os momentos, em particular, quando exigido pela EY. Isso inclui manter documentação, realizar revisões regulares e cooperar com a EY em auditorias ou avaliações relacionadas à proteção de dados.

Protegendo Dados Durante o Ciclo de Vida do Serviço

Para garantir o manuseio responsável dos Dados durante a prestação de serviços à EY, os Fornecedores são obrigados a seguir recomendações específicas. Essas recomendações (ou diretrizes) são estruturadas em três fases principais do ciclo de vida do serviço, a saber:

1

Início do Serviço

1

No início de qualquer serviço, os Fornecedores devem tomar medidas proativas para estabelecer um ambiente de Dados seguro e em conformidade:

Classificação de Dados: Compreender a natureza e a sensibilidade dos Dados a serem tratados, incluindo sua classificação (por exemplo, confidencial, pessoal, sensível, público).

Minimização de Dados: Identificar e coletar apenas os Dados estritamente necessários para a prestação dos serviços.

Definição de Propósito: Definir claramente o propósito para o qual os Dados serão tratados, garantindo alinhamento com as instruções e termos contratuais da EY.

Controles de Acesso: Implementar acesso baseado em funções aos Dados, limitando a exposição apenas ao pessoal autorizado.

Acordos de Tratamento de Dados ("Data Processing Agreements" ou "DPAs"): Garantir que todas as cláusulas de proteção de Dados aplicáveis ou um DPA específico sejam incluídos nos acordos e que contratados ou subcontratados, se houver, estejam vinculados por obrigações equivalentes.

Planejamento de Segurança: Estabelecer medidas técnicas e organizacionais apropriadas para proteger os Dados contra qualquer Incidente de Dados.

Métodos de Transferência: Avaliar e aplicar métodos de transferência seguros (por exemplo, e-mail criptografado, protocolos seguros de transferência de arquivos, ferramentas de transmissão da EY) apropriados ao tipo de Dados e ao nível de risco.

Consulta e Esclarecimento: Entrar em contato com seu contato designado na EY para esclarecer quaisquer dúvidas sobre os requisitos de manuseio de Dados, protocolos de transferência ou expectativas de conformidade. A comunicação aberta nesta fase é essencial para garantir o alinhamento e evitar o gerenciamento inadequado dos Dados.

2

Durante o Serviço

Durante a prestação do serviço, os Fornecedores devem manter práticas robustas de proteção de Dados e monitorar a conformidade:

2

Tratamento Seguro
Os Fornecedores devem aplicar as medidas de segurança e proteção de dados definidas durante a fase inicial do serviço. Todos os Dados devem ser tratados de acordo com os métodos de transmissão, controles de acesso e protocolos de segurança previamente acordados com a EY. Qualquer desvio desses padrões deve ser aprovado pelo seu contato designado na EY. A EY não será responsável por quaisquer desvios ou por qualquer não conformidade com a Lei Aplicável resultante das ações do Fornecedor.

Monitoramento e Auditoria
Realizar revisões internas periódicas para verificar se as práticas de manuseio de Dados permanecem em conformidade com os requisitos da EY e as Leis Aplicáveis. As descobertas devem ser documentadas e ações corretivas tomadas prontamente.

Monitoramento de Acesso a Dados
Monitorar continuamente quem tem acesso aos Dados e garantir que o acesso seja limitado a indivíduos com uma necessidade legítima de negócios. Qualquer alteração no pessoal ou nas funções deve ser refletida nas permissões de acesso imediatamente.

Gestão de Incidentes
Manter um processo documentado para identificar, relatar e responder a Incidentes de Segurança com Dados. Em alguns casos, a EY deve ser notificada imediatamente sobre Incidentes de Segurança de acordo com as obrigações contratuais e legais.

Treinamento e Conscientização
Garantir que todo o pessoal (por exemplo, empregados dos Fornecedores, representantes legais e contratados) envolvido no tratamento de Dados seja treinado nos princípios de proteção de dados e nos requisitos específicos da EY.

Conclusão do Serviço

No final dos serviços, os Fornecedores devem garantir que os Dados sejam tratados adequadamente para evitar riscos residuais:

▸ **Devolução ou Exclusão de Dados:** Após a conclusão do serviço, os Fornecedores devem devolver todos os Dados à EY de acordo com as obrigações contratuais e as instruções da EY. Se não for necessária a devolução, por exemplo, quando se tratar de Dados manipulados em ambientes eletrônicos, ou uma vez que a devolução tenha sido concluída, os Fornecedores devem proceder com a exclusão segura de todos os Dados de seus sistemas.

▸ **Revogação de Acesso e Limpeza de Dados:** Remover quaisquer direitos de acesso desnecessários a quaisquer sistemas, plataformas ou repositórios de Dados. Garantir que todos os Dados residuais armazenados localmente ou em ambientes de nuvem sejam excluídos de forma segura e não possam ser recuperados.

▸ **Confirmação Formal:** A menos que outra forma especificada no contrato firmado, fornecer à EY uma confirmação formal da devolução ou exclusão dos Dados. Isso pode incluir certificados de destruição segura, registros assinados ou outra documentação verificável que demonstre conformidade com os requisitos de manuseio de Dados da EY.

▸ **Revisão Pós-Serviço:** Realizar uma revisão final para garantir que nenhum Dado permaneça nos sistemas ou backups do Fornecedor.

▸ **Políticas de Retenção:** Garantir que nenhum Dado seja retido além do período de retenção acordado, a menos que seja legalmente exigido.

▸ **Não Reutilização de Dados:** Os Dados obtidos durante o relacionamento não devem ser reutilizados para qualquer outro propósito ou projeto, a menos que a autorização por escrito explícita tenha sido obtida da EY. A reutilização não autorizada constitui uma violação das obrigações contratuais e legais.

3

Diretrizes Adicionais sobre Segurança e Proteção de Dados

As seguintes recomendações visam reforçar as práticas de segurança de Dados em todas as etapas da prestação de serviços. Os Fornecedores devem aderir a essas diretrizes além dos princípios gerais e recomendações de ciclo de vida descritos neste documento.

Solicitações de Titulares de Dados

- Notifique imediatamente seu contato designado na EY ao receber qualquer solicitação de um Titular de Dados (por exemplo, acesso, retificação, exclusão de Dados), a menos que o Fornecedor seja responsável pelo tratamento e pelo cumprimento dessa obrigação (ou seja, o Fornecedor atua como um controlador de Dados independente de acordo com a Lei Aplicável).

- Não responda ou compartilhe quaisquer Dados sem autorização por escrito explícita da EY, a menos que seja legalmente exigido.

- Esteja preparado para apoiar a EY no cumprimento dos direitos dos Titulares de Dados de maneira oportuna e em conformidade.

Incidentes de Segurança com Dados

- Relate imediatamente ao seu contato designado na EY qualquer Incidente de Segurança com Dados confirmado ou suspeito, violações ou vulnerabilidades de segurança.

- Não divulgue detalhes do Incidente de Segurança com Dados a terceiros, a menos que explicitamente autorizado pela EY, a menos que seja legalmente exigido.

- Siga os protocolos de resposta a Incidentes de Segurança com Dados da EY e coopere plenamente nas investigações e esforços de remediação.

- Em algumas jurisdições, a comunicação de um Incidente de Segurança com Dados é exigida para os Titulares de Dados aplicáveis e até mesmo para as Autoridades de Supervisão de Proteção de Dados, no Brasil, **Agência Nacional de Proteção de Dados ("ANPD")** os requisitos da Lei Aplicável devem ser seguidos.

Uso de Ferramentas Tecnológicas

- O uso da tecnologia deve estar alinhado com as leis, regulamentos e requisitos aplicáveis da EY.

- A tecnologia, incluindo aquelas com inteligência artificial ("IA"), deve ser usada para apoiar – não substituir – a experiência profissional, as responsabilidades e os padrões éticos do fornecedor ao prestar serviços à EY.

- Espera-se que o Fornecedor se mantenha informado sobre os riscos, limitações e capacidades em evolução das tecnologias emergentes para garantir o uso responsável e eficaz sem gerar qualquer preocupação ou responsabilidade à EY.

Práticas de Segurança

- Sempre verifique os destinatários e anexos de e-mails antes de enviar mensagens contendo Dados.

- Evite encaminhar Dados para contas de e-mail pessoais ou destinatários não autorizados.

- Mantenha a segurança física de dispositivos portáteis (por exemplo, laptops, unidades USB); evite deixá-los ligados ou sem supervisão.

- Evite o acesso não autorizado a dispositivos de trabalho bloqueando telas e usando senhas fortes.

- Evite discutir assuntos confidenciais em ambientes públicos ou não seguros.

- Ao trabalhar remotamente, garanta que o espaço de trabalho seja privado e seguro, e use ferramentas aprovadas e redes seguras.

- Evite imprimir ou transportar documentos físicos, a menos que seja estritamente necessário, e proteja documentos físicos contra acesso não autorizado, especialmente ao trabalhar fora do escritório.

- Aplique senhas fortes e autenticação multifator ("MFA") aos seus sistemas e não compartilhe credenciais de sistema ou tokens de acesso com outros.

Redes e Controle de Acesso

- Valide a legitimidade das redes Wi-Fi públicas antes de se conectar; prefira redes protegidas por senha e use VPNs quando disponíveis.

- Aplique o princípio do “necessário saber” ao compartilhar Dados, limitando o acesso apenas àqueles que precisam dele para a prestação de serviços.

- Realize revisões periódicas das permissões de acesso a plataformas colaborativas e repositórios de Dados.

Definições

Lei Aplicável: Qualquer lei, regra, regulamento ou diretiva, incluindo, mas não se limitando às questões de privacidade e proteção de dados, aplicável ao Fornecedor, como a **Lei Geral de Proteção de Dados Pessoais ("LGPD").**

Dados: Este termo é usado de forma ampla para se referir tanto a Dados Pessoais quanto a outros tipos de Informações Confidenciais - como informações de terceiros, informações de clientes e informações comerciais da EY -, conforme definido pelas Leis Aplicáveis e pelas políticas, procedimentos e padrões internos da EY.

Titular de Dados: O indivíduo a quem as informações coletadas e tratadas se referem, conforme definido pela Lei Aplicável.

Informações Confidenciais: Qualquer informação relacionada à EY e seus clientes tratada de acordo com um acordo com a EY. Informações de Clientes significam qualquer informação relacionada aos assuntos de um cliente atual ou anterior obtida pela EY de um cliente ou de um terceiro em conexão com um engajamento com tal cliente. Por outro lado, Informações da EY significam (i) Dados Pessoais; (ii) informações de terceiros; (iii) informações de clientes; e (iv) informações comerciais da EY.

Incidente de Segurança com Dados: Qualquer evento que comprometa a segurança, confidencialidade, integridade ou disponibilidade de qualquer Dado, incluindo qualquer divulgação, perda, uso, destruição, alteração ou acesso não autorizado ou inadequado aos Dados.

Dados Pessoais: Significa (i) qualquer informação que, sozinha ou em conjunto com qualquer outra informação, se refira a uma pessoa natural identificada ou identificável (como nome, número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural), e (ii) qualquer outra informação considerada como informação pessoalmente identificável, dados pessoais ou informações pessoais (ou termo similar) sob a lei aplicável.

Dados Pessoais Sensíveis: Refere-se a Dados Pessoais que, de acordo com a lei aplicável, são considerados sensíveis devido ao seu potencial de afetar a privacidade do Titular de Dados ou levar à discriminação. Isso inclui, mas não se limita a, dados que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos usados para fins de identificação, dados relacionados à saúde e dados sobre a vida sexual ou orientação sexual de uma pessoa natural. Além disso, Dados Pessoais relacionados a condenações e infrações criminais, bem como Dados que possam facilitar o roubo de identidade ou fraude de pagamento (como números de contas financeiras, detalhes de cartões de crédito e números de identificação emitidos pelo governo), são considerados sensíveis, na medida definida pela lei aplicável.

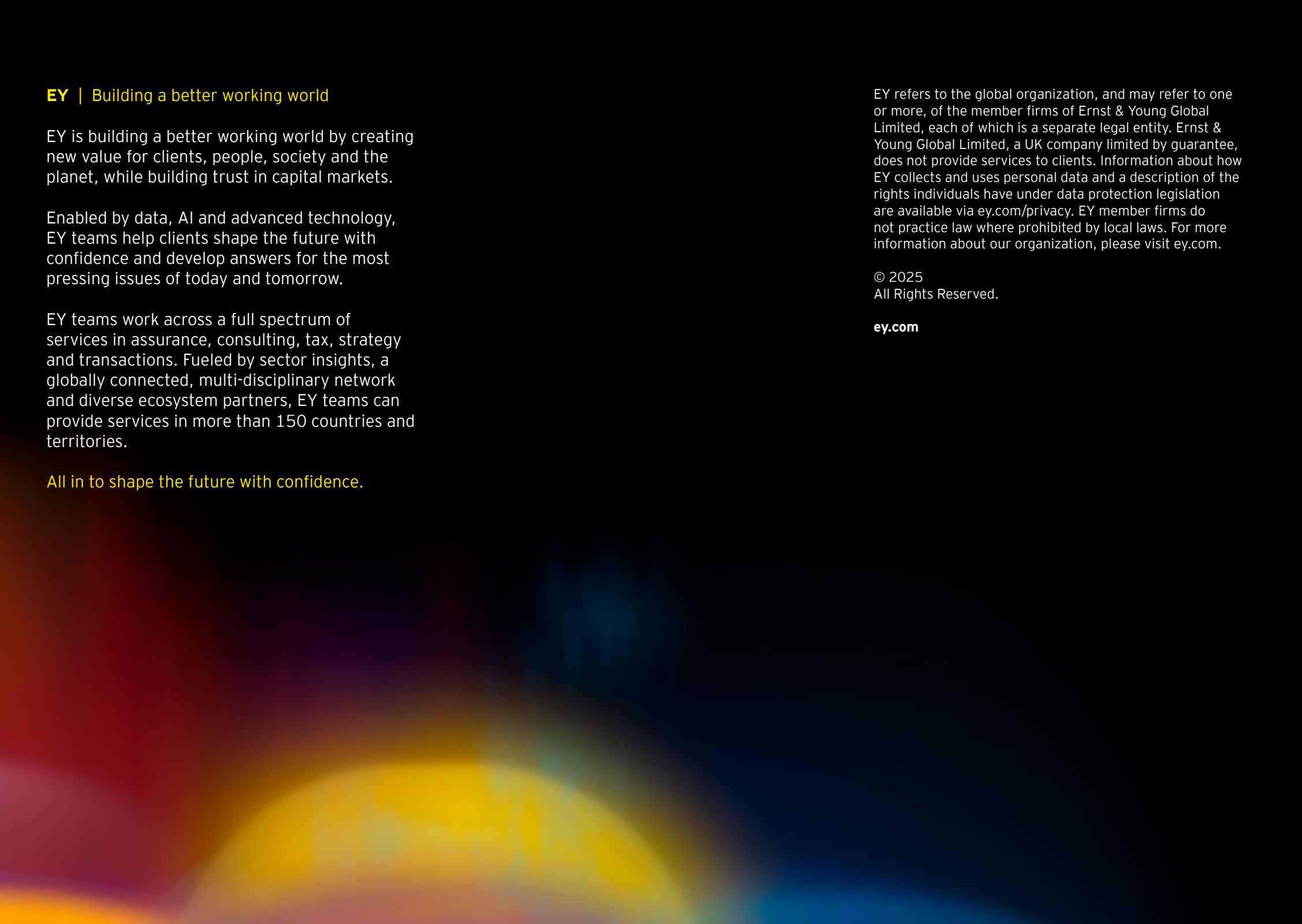
EY | Building a better working world

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