

LEI GERAL DE PROTEÇÃO DE DADOS





Looplex



Guia para Terceiros

Introdução

A nova **Lei Geral de Proteção de Dados (LGPD)** aborda um de nossos mais importantes princípios: a transparência no relacionamento com nossos clientes.

Ela incentiva a modernização e a implementação de programas de segurança e governança para o tratamento adequado de dados pessoais.

Preparamos essa cartilha para uso interno e para nossos parceiros Looplex, com toda a documentação necessária para a atualização dos contratos atualmente em vigor. A atualização terá a formalização das responsabilidades e clareza de papéis de ambos controlador e operador de dados, conforme definido pela própria LGPD.

A Lei nº 13.709/18, também conhecida como Lei Geral de Proteção de Dados (LGPD), é o principal marco regulatório que trata sobre o tema no Brasil.

Inspirada na General Data Protection Regulation (GDPR), a regulação europeia de proteção de dados, a LGPD irá agregar às normas já existentes ao entrar em vigor.

Ela introduz um sistema de regras sobre tratamento de dados pessoais em situações em que os dados são coletados, tratados ou utilizados para operações e ofertas de bens ou serviços que aconteçam em território nacional. Impacta todos os setores da economia, inclusive a advocacia.

A lei tem como objetivo criar um ambiente de maior controle sobre os dados pessoais para os indivíduos, e de maiores responsabilidades para as organizações que tratam esses dados. Ela reconhece a importância de direitos essenciais para o exercício de atividades econômicas e o desenvolvimento do bem-estar da própria sociedade.

Além do respeito à privacidade e sua não violação, a LGPD estabelece como fundamento da proteção de dados a liberdade de expressão, de informação, de comunicação e de opinião, bem como o desenvolvimento econômico e tecnológico, a inovação, a livre concorrência e a livre iniciativa.

PERGUNTAS E RESPOSTAS

Separamos algumas perguntas frequentes sobre privacidade e proteção de dados pessoais relativas à LGPD, para entendimento dos seus conceitos e nosso papel



Faq 1: O que é um “controlador” e o que é um “operador”?

O **controlador** é responsável pela tomada de decisões em relação: (i) a como os dados pessoais serão utilizados e tratados; (ii) ao objetivo ou ao resultado do tratamento dos dados pessoais; (iii) a quais dados pessoais devem ser usados.

O **operador** é contratado para realizar atividade que envolva dados pessoais em nome do controlador e deverá seguir as instruções do controlador sobre o tratamento dos dados. O operador não tem autorização para tratar os dados pessoais de forma diferente da que está prevista em contrato e não decide quais dados pessoais serão tratados e para quais finalidades.

Para cada processo de negócios, é preciso determinar qual posição a organização ocupa; se controlador ou operador de dados, já que a função que exercer será importante para a definição de responsabilidades e obrigações. Uma empresa pode ocupar a posição de controlador em uma atividade e, ao mesmo tempo, ocupar uma posição de operador em outra atividade.

É importante reconhecer os riscos envolvidos em relação a um operador de dados:

- Os **operadores** de dados devem tratar os dados pessoais seguindo estritamente as instruções dadas pelos controladores.
- Os **controladores** devem exigir garantias de que os dados pessoais estão sendo tratados pelos operadores de acordo com as suas instruções. Exemplos dessas garantias são: formalização de um acordo de tratamento de dados pessoais; exigência de que os operadores obedeçam a determinados padrões técnicos; possibilidade de realização de auditorias, entre outras.
- O operador de dados pode contratar um terceiro para tratar os dados pessoais em seu nome, sendo esse o **suboperador**, desde que

não haja proibição em contrato. Ao contratá-lo, o operador deve firmar um contrato com disposições que garantam o mesmo nível de proteção de dados pessoais existente no tratamento realizado pelo operador, se responsabilizando integralmente pela atuação do suboperador.



Faq 2: O que são “dados pessoais”?

Dados pessoais são informações relacionadas a uma pessoa natural identificada ou identificável (ou seja, o titular dos dados). Dependendo do contexto, um dado que, a princípio, não parece identificar um indivíduo pode, em conjunto com informações distintas levar a identificá-lo. São exemplos: endereços IP; dados de localização; número de registro de empregado ou até mesmo um identificador único (UID).

Exemplo prático: quando um pedaço de papel contém o número “2.000” isoladamente, essa indicação é apenas um número. Porém, se esse documento for um comprovante de salário associado a um nome, conta bancária e número de previdência social, o número indicativo do salário passa a ser um dado pessoal em seu conjunto.

A Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) define, ainda, **dado pessoal sensível**, que são os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, e dados genéticos ou biométricos, quando vinculados a uma pessoa natural. Os dados pessoais sensíveis exigem uma atenção especial quando forem tratados, pois nem todas as bases legais podem ser utilizadas neste caso.



Faq 3: O que é tratamento de dados pessoais?

São operações realizadas com dados pessoais - desde a coleta dos dados até a destruição no final de seu ciclo de vida – o que inclui as ações intermediárias, como produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.



Faq 4: E quanto ao direito de livre acesso aos dados pessoais?

Todo titular de dados pode pedir para o controlador de seus dados pessoais: (i) a confirmação da existência de tratamento; (ii) o acesso aos seus dados; (iii) a correção de dados incompletos, inexatos ou desatualizados; (iv) a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desacordo com a lei; (v) a portabilidade dos dados a outro fornecedor; (vi) a eliminação dos dados pessoais tratados com consentimento do titular; (vii) informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (ix) a revogação do consentimento.



Faq 5: Quais os impactos de um incidente de segurança que envolva dados pessoais?

A organização deverá adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais de acessos

não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Isso, porque a organização tem a obrigação de garantir a segurança da informação.

Caso ocorra algum incidente de segurança que envolva dados pessoais, caberá ao controlador comunicar à autoridade nacional e ao titular dos dados pessoais a ocorrência do incidente de segurança que possa acarretar riscos ou danos relevantes aos titulares.



Faq 6: O que é relatório de impacto à proteção de dados [DPIA]?

O relatório de impacto à proteção de dados [DPIA] é uma ferramenta usada para identificar e reduzir os riscos de privacidade em qualquer projeto, processo ou programa. Um DPIA não é uma avaliação única. Pelo contrário, é um “documento vivo” usado para registrar a identificação e mitigação de riscos de privacidade em diferentes momentos no ciclo de vida de um projeto ou programa ou novos processos.



Faq 7: O que é o “Privacy by Design”?

É um documento pensado para auxiliar que novos processos, projetos, produtos e serviços que envolvam o tratamento de dados pessoais, estejam de acordo com a proteção de dados e privacidade. É importante que ele seja preenchido no início dessas iniciativas pois fornece orientações para garantir o cumprimento à legislação e regulamentação de proteção de dados que se aplicam à organização.

COMO ISSO IMPACTA A LOOPLEX E NOSSO RELACIONAMENTO COM OS CLIENTES?

Precisamos pensar nos reflexos da LGPD perante nossos clientes de um lado e perante nossa equipe e parceiros de outro



Impacto em nossos produtos e relacionamento com clientes

Perante nossos clientes somos apenas **operadores** dos dados, pois não temos controle ou qualquer poder decisório sobre o que é coletado ou mesmo sobre qual é a utilização dada pelo escritório de advocacia ou departamento jurídico em relação aos dados processados nos Templates de lógica jurídica desenvolvidos pelos engenheiros jurídicos.

Por isso, o processamento dos dados é feito exclusivamente de acordo com as regras de negócio de nosso sistema, conforme indicado nos [Termos de Uso](#) e [Política de Privacidade](#). Qualquer tratamento diferente precisa ocorrer mediante instrução escrita do cliente (por exemplo uma edição diretamente no banco de dados, ou um relatório de BI customizado).

Além disso, não podemos compartilhar dados de nossos clientes com terceiros que não tenham sido anonimizados sem o seu expresso consentimento, que pode ser dado diretamente na interface (“click wrap”), sempre com clareza para o usuário sobre o que ele está consentindo.

Além disso, internamente, nomeamos um *Data Protection Officer* que observará, juntamente com o CEO, a observância da LGPD nas rotinas internas de segurança e no acesso a dados de cliente pela nossa equipe.

Dentro da Looplex, as funcionalidades disponíveis de controle de privacidade dos dados e autorizações de compartilhamento já são suficientes para que possamos atender a LGPD na qualidade de **controladores**, perante clientes e colaboradores.

Estamos treinando nossa equipe de suporte e engenharia jurídica para que eles possam assessorar nossos clientes nessa transição.



Impacto no relacionamento com parceiros e com nossa equipe

Para nossos parceiros, estamos auditando todos nossos contratos para ter certeza que eles estão em conformidade com a LGPD, por exemplo explicitando a cadeia de custódia dos dados do cliente em nossas integrações.

Contratos que tenham alguma incompatibilidade precisam ser aditados e atualizados.

E para a nossa própria equipe, implementamos na administração controles mais rígidos de acesso e regras de uso dos dados pessoais de nossos consultores, funcionários e terceirizados. Dados pessoais sensíveis de nossos colaboradores agora estão sujeitos às proteções e tratamentos da LGPD.

looplex.com.br

Rua da Consolação, 2302 - Consolação
01302-001 – São Paulo/SP

