Guia sobre LGPD

O que é a LGPD?

A Lei nº 13.709/18, também conhecida como "LGPD" ou Lei Geral de Proteção de Dados estabelece regras sobre a coleta, armazenamento, compartilhamento ou qualquer outra forma de tratamento de dados pessoais, garantindo mais direitos às pessoas físicas titulares dos dados e impondo mais obrigações e penalidades em caso de não cumprimento pelas empresas que usam dados pessoais.

Quais os princípios da LGPD?

- Finalidade: Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
- Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
- Necessidade: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.;
- Livre acesso: Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
- Qualidade dos dados: Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
- Transparência: Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
- Segurança: Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.;
- Não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
- Responsabilização e prestação de contas: Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Quais os principais pontos apresentados pela LGPD?

- Os dados pertencem ao titular dos dados e não às empresas que os coletam, armazenam ou tratam.
- A LGPD coloca em destaque a necessidade de transparência no tratamento do dado.
- Segurança da informação e boas práticas da prevenção de vazamento e de uso indevido dos dados pessoais e maior controle de acesso e rastreabilidade de como dados está sendo utilizado e acessado pela empresa.
- Os princípios da LGPD devem ser observados, como apenas usar os dados para finalidades legítimas e coletar e usar o mínimo de dados necessário para cumprir os objetivos das empresas.
- Garantia de direitos aos titulares, como de acessar os seus dados pessoas e de pedir informações sobre o seu tratamento.

Quem é afetado pela LGPD?

Serão impactadas pela LGPD todas as empresas que usam quaisquer tipos de dados pessoais, além do setor público. É importante lembrar que a lei engloba dados digitais, os dados coletados em papel, como fichas de cadastro e cupons de promoções ou mesmo coletados por outros meios, além de dados acessíveis publicamente, independente do formato.

Quais são os papéis e responsabilidades definidos na LGPD?

A LGPD define os quatro principais envolvidos quando se trata de proteção de dados pessoais:

1. O titular – é a pessoa física a quem se referem os dados pessoais, como, por exemplo, as pessoas físicas com a intenção de contratar um crédito consignado e os empregados do Correspondente;
2. O operador – deve tratar dados apenas de acordo com as orientações do controlador dos dados, como é o caso da loja (PJ), quando trata os dados de um cliente ou potencial cliente do banco, sendo o operador responsável pela coleta e uso de dados pessoais de acordo com a LGPD e sua efetiva segurança da informação;
3. O controlador – é a quem cabe tomar as decisões sobre o tratamento dos dados pessoais. O banco Itaú Correspondente é considerado controlador e receberá os dados do titular que sejam coletados pelo correspondente. Cabe ao controlador garantir o atendimento aos direitos do titular, além de realizar o tratamento de acordo com a LGPD e cumprir outras obrigações previstas na LGPD, como a de elaboração do relatório de impacto à proteção de dados pessoais, quando necessário. O Correspondente é também considerado controlador de dados pessoais quando toma decisões a respeito dos dados pessoais ou quando atua em desacordo com as instruções do banco. De qualquer forma, o Correspondente deve auxiliar o banco no atendimento dos direitos dos titulares e na elaboração de relatórios de impacto ou outros documentos exigidos pela LGPD, devendo fornecer as informações solicitadas pelo Itaú a fim de preencher o relatório. O relatório de impacto poderá ser requisitado a qualquer tempo pela ANPD. Nos casos onde o Corban é o controlador (quando de

forma independente realiza a coleta de dados de outras fontes/bases de dados e quando toma as decisões sobre o uso dos dados) este é o único responsável por atender a LGPD.

4. O encarregado – É o profissional designado pelo controlador e pelo operador para atuar como canal de contato com a Autoridade Nacional de Dados Pessoais e os titulares, respondendo pela de proteção dos dados do correspondente.

A LGPD permite que haja apenas um encarregado por CNPJ/Grupo, porém quando falamos de lojas substabelecidas, a fim de obter o melhor controle no fluxo das informações, é interessante que tenha um encarregado para cada.

Quais são as funções e responsabilidades do Encarregado de Dados?

O Encarregado de proteção de dados é responsável pela governança de proteção dos dados pessoais na empresa:

- Informar e aconselhar a empresa e os seus funcionários sobre as suas obrigações em relação à LGPD;
- Monitorar a conformidade com a LGPD. Isso inclui supervisionar documentação, processos e registros
- Atuar como um ponto de contato para solicitações dos titulares dos dados com relação ao tratamento de seus dados pessoais e ao atendimento de seus direitos;
- Cooperar com a autoridade de proteção de dados (ANPD – Autoridade Nacional de Proteção de Dados) e atuar como um ponto de contato em questões relativas ao tratamento de dados pessoais na organização.

O que são dados pessoais?

Todas as informações que permitem identificar ou tornam uma pessoa física identificável. Alguns exemplos são: nome, números de documento (RG e CPF), dados de localização, dados profissionais, dados de crédito e financeiros (ex. nº da operação), perfis e endereços eletrônicos.

Alguns dados pessoais são considerados sensíveis pela lei e possuem mais restrições no tratamento, de modo a evitar práticas discriminatórias. Por exemplo, os dados que se referem à origem étnica ou racial da pessoa, suas convicções políticas e religiosas, filiação a sindicatos ou organizações políticas, filosóficas ou religiosas, dados genéticos e dados ligados à saúde e vida sexual da pessoa. Também são considerados sensíveis os dados biométricos da pessoa.

É importante lembrar que nem toda informação é considerada dado pessoal, mas o conceito previsto na LGPD é amplo e deve ser avaliado o tipo de dado e o contexto do tratamento.

Quais são os principais direitos do titular dos dados, e como os dados pessoais devem ser tratados?

O titular tem direito de requerer do controlador: a confirmação de que seus dados pessoais são tratados, além de acessar, pedir a correção, exclusão e portabilidade dos dados pessoais que as empresas têm sobre ele. Além disso, o titular também tem direito a obter informações sobre o tratamento e se houve compartilhamento dos seus dados.

Todos os tratamentos devem ter algum respaldo legal na LGPD para que possam ser realizados. Algumas das possibilidades de tratamento (também conhecidas como "bases legais") são obrigação legal, execução de contrato, proteção do crédito, consentimento e legítimo interesse. O consentimento tem que livre (o titular pode concordar ou não), destacado das demais cláusulas contratuais, inequívoco (deve-se ter certeza de que o titular concorda com o tratamento) e específico (indicar as finalidades de uso). Além disso o titular pode retirar esse consentimento a qualquer momento.

Quais são as obrigações das empresas?

As empresas não poderão mais tratar dados pessoais sem respaldo legal na LGPD, devendo ser garantida transparência ao titular sobre esses tratamentos. O titular pode ser qualquer pessoa a quem o dado se refere, independente do relacionamento das empresas com essa pessoa. Além disso, as empresas são responsáveis por monitorar e garantir a segurança dos dados, impedir vazamentos e acessos ou usos indevidos. É necessário também registrar as atividades de tratamento, ou seja, ter um inventário de tratamento de dados no qual constem as informações sobre os dados pessoais tratados, os titulares, a finalidade do tratamento, com quem é compartilhado, quando tempo o dado é retido e qual a base legal que respalda esse tratamento. Para os tratamentos definidos como legítimo interesse ou de alto risco, também deve ser feito o relatório de impacto à proteção de dados pessoais.

Além disso as empresas devem definir processo para atender os direitos de todos os titulares e permitir a revogação do consentimento, quando necessário.

Quais sanções previstas na LGPD caso eu não me adeque?

As penalidades pelo descumprimento da LGPD, a serem aplicadas pela ANPD incluem:

- Multa, simples e diária, de até 2% (dois por cento) do faturamento da pessoa jurídica, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- Advertência e publicização da infração;
- Bloqueio ou eliminação de dados pessoais;

- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a i
- infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Impacto da LGPD no Corban modelo Call Center

Para bases fornecidas pelo Itaú Correspondente, a oferta do produto estará respaldada pelo legítimo interesse. Com relação às bases adquiridas ou repassadas por terceiros, antes de ofertar o produto para o cliente, será necessário ter a autorização do titular para o uso e armazenamento dos dados. Outro ponto importante é que esses dados, uma vez coletados devem estar relacionados ao serviço prestado pela empresa e autorizado a receber ofertas de produtos ou serviços.

Caso o cliente solicite o opt-out da oferta, este não deverá mais receber ligações com oferta do consignado e deve ser orientado a ligar na Central Cliente para solicitar a exclusão de seus dados.

O lado positivo dessa mudança é que como os contatos precisarão optar claramente por receber suas campanhas, somente os clientes em potencial mais envolvidos provavelmente permanecerão em seus bancos de dados. Você comunicará apenas aos clientes e prospects mais valiosos, aqueles que realmente querem ouvir e comprar com você.

Como solicitar o consentimento?

Orientamos que ao iniciar a conversa seja perguntado ao cliente se ele aceita ou não ouvir a oferta que o correspondente deseja realizar.

O consentimento para bases adquiridas ou repassadas por terceiros, é essencial para seguir de acordo com as normativas da LGPD.

Caso o cliente procure a loja para contratar o empréstimo consignado, neste caso, não é necessário o consentimento, a base legal é a execução do contrato (contrato de empréstimo/financiamento do cliente com a IF).

O que é preciso fazer para se adequar a LGPD?

1. **Antes de mais nada:**

- A principal atitude é não utilizar base ou lista de dados de titulares de origem ilegal (por exemplo, adquirir as informações em mercados paralelos ou de origem duvidosa) e ter respaldo na LGPD para coleta e uso das informações. Os dados que sejam fornecidos pelo banco não devem ser compartilhados com terceiros ou usados para outras finalidades.

- Nomear e divulgar o Encarregado de Dados (DPO) nos canais de comunicação (por exemplo: site). O Encarregado poderá ser qualquer funcionário da empresa, devidamente treinado para atender as solicitações de clientes e órgão regulador.
- Adotar medidas de segurança da informação e de proteção de dados, de modo a evitar incidentes de segurança e usos ou acessos não autorizados.

2. Conhecer os dados

Identificar quais dados pessoais a empresa tem, como são coletados, onde estão armazenados através do registro de atividades de tratamento e, quando necessário, por meio do Relatório de impacto à proteção de dados pessoais:

- Mapear todos os processos que têm a coleta, o uso e compartilhamento de dados pessoais, podendo ser dados de clientes, colaboradores ou outros titulares de dados. Exemplo: Quais são os dados pessoais, a origem dos dados, compartilhamento com áreas internas e empresas externas, armazenamento, finalidade de uso dos dados, quando o titular do dado tem o conhecimento de uso dos seus dados etc.
- O titular do dado deve estar ciente de que suas informações serão utilizadas para o fim específico, neste caso a contratação de crédito consignado. Caso a base legal seja consentimento, a autorização deve ser formalizada pelo titular dos dados, de forma escrita, falada ou digitada, através de formulários. Além disso deve ser estabelecido um processo para ele revogar esse consentimento a qualquer momento. Se a base legal for o legítimo interesse para a realização da oferta, deve ser garantida a possibilidade do cliente não mais receber tais ofertas;
- Revisão de contratos de prestadores de serviços para prever condições sobre o uso e tratamento das informações.

3. Gestão de como os dados pessoais são utilizados, acessados e armazenados.

Além de controlar quais dados são coletados, armazenados e utilizados, é necessário identificar quais as pessoas possuem acesso a eles e como estão sendo utilizados. Para isso, a empresa deve ter visibilidade de como estes são usados em seu ambiente, implementando procedimentos padronizados e fluxos de trabalho para lidar com os dados pessoais, além de restringir o acesso apenas para quando os funcionários necessitem da informação para executar suas funções.

- Fluxo de exclusão e atualização das informações caso o titular dos dados solicite, desde que autorizado pelo controlador.
- Criação de políticas e procedimentos de uso e proteção de dados;
- Armazenamento seguro das informações utilizando ferramentas para este fim, por exemplo, armazenamento em nuvem (cloud) ou em banco de dados na rede interna com a devida segurança e controles de acesso;
- Criação de perfis de acesso aos dados para limitar o acesso somente aos usuários autorizados;
- Consulta e guarda da informação quando o corban usa outros meios de gestão além do IBConsig, por exemplo sistemas próprios (Domus, FINAZ, Mola, etc.).

4. Armazenamento do físico.

- Ter local onde os documentos serão guardados enquanto não são enviados às filiais;
- Restringir o acesso aos documentos físicos;
- Descarte adequado dos documentos físicos de operações canceladas e que não serão necessários o envio dos documentos físicos ao banco, por exemplo "destruir" os documentos físicos através de máquina fragmentadora;
- Processo de envio dos documentos às filiais para mitigar o risco de extravio, por exemplo não enviar os documentos via Correios, conforme orientação do time de Formalização.

5. Definir controles de segurança para prevenir, identificar e responder às vulnerabilidades e vazamento de dados.

- Criação de políticas de armazenamento e acesso aos dados dos titulares;
- Criação de procedimentos operacionais e técnicos para prevenir o acesso e compartilhamento indevido e vazamento dos dados pessoais.

6. Correspondente bancário e a LGPD, como agir?

- Manter-se informado sobre as constantes atualizações dos processos, a fim de revisá-los e aprimorá-los sempre.
- Bases fornecidas por outras IFs não devem ser utilizadas. Mesmo consentida a oferta do consignado, uma vez que o titular forneceu seus dados para uma instituição, utilizá-los em outro local pode ser considerado vazamento de informação.