Diretrizes - Lei Geral de Proteção de Dados (LGPD)

Banco Santander

Conteúdo

O que é a LGPD

Inspirada na GDPR, legislação de proteção de dados europeia, criada em 1995 e atualizada em 2018, a Lei Geral de Proteção de Dados, mais conhecida como LGPD, é uma lei que foi criada para regular os tratamentos de dados pessoais seja no meio digital ou físico.

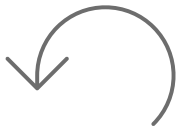
Na LGPD estabelece-se as regras mínimas para utilização dos dados de pessoas naturais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

São considerados tratamentos de dados, todas as atividades abaixo, quando feitas com dados pessoais:

- Coleta
- Produção
- Recepção
- Classificação
- Utilização
- Acesso
- Reprodução
- Transmissão
- Distribuição
- Processamento
- Arquivamento
- Armazenamento
- Eliminação
- Avaliação da informação
- Controle da informação
- Modificação
- Transferência
- Difusão
- Extração

Princípios da LGPD

Finalidade: propósitos legítimos, específicos, explícitos e informados



Adequação: compatível com as finalidades

Necessidade: utilização apenas de dados estritamente necessários

Livre acesso: acesso ao tratamento e à integralidade dos dados

Qualidade dos dados: dados exatos claros, relevantes e atualizados

Transparência: Informações claras e precisas

Segurança: medidas técnicas e administrativas aptas a proteger os dados pessoas

Prevenção: adoção de medidas para evitar danos aos titulares

Não discriminação: não utilização para fins discriminatórios, ilícitos ou abusivos

Responsabilização e prestação de contas: demonstração de adoção de medidas eficazes ao cumprimento das normas.

A quem se aplica

Aplicada à qualquer pessoa física, empresa, entidade pública ou privada que realize coleta e tratamento de informações.

Pessoa física

Entidade pública ou privada

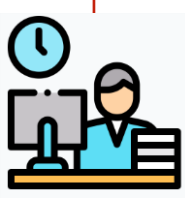
A LGPD não se aplica ao tratamento de dados realizados para fins exclusivamente particulares e não econômicos, jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança de Estado, de investigação ou repressão de infrações penais, entre outros.

Partes envolvidas

Titular
Dono do dado

Operador
Realiza o tratamento de dados pessoais em nome do controlador

Controlador
Toma decisão sobre o tratamento do dado



Encarregado
Pessoa indicada pelo controlador e o operador como canal de comunicação entre Controlador, Titular e ANPD

ANPD
Autoridade Nacional de Proteção de Dados

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Note que uma mesma pessoa pode ser controlador e operador simultaneamente;

Encarregado: pessoa indicada para atuar como canal de comunicação. A GDPR chama de DPO – Data Protection Officer

ANPD: tratar o tema de proteção de dados, editando regras gerais, fiscalizar o cumprimento da Lei e aplicar sanções.

Dado pessoal

Dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável.

Dados identificados: são aqueles que, diretamente, conseguem identificar o titular. Exemplos: Nome, RG/CPF, CNH, CTPS, PIS/NIS e etc.

Dados identificáveis: são aqueles que não permitem a identificação direta do titular, mas, em conjunto com outras informações é possível atingir esse objetivo. Exemplos: Idade, número de telefone, nacionalidade, nome da mãe, nome do pai, endereço residencial e dado biométrico.

Dado pessoal sensível

Dado pessoal sensível são os dados que entram numa esfera mais íntima e privada do indivíduo.

São dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação à sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde e ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Esse tipo de dado merece um grau maior de proteção, pois pode causar a discriminação do indivíduo.

Dado anonimizado

É o dado relativo ao Titular que não pode ser identificado.

Exemplo: estudo sobre estado civil apresenta resultado que 10% das mulheres na faixa etária de 35 a 40 anos, que moram em São Paulo são divorciadas. Não é possível identificar essas mulheres.

Anonimização

É a utilização de meios técnicos para o tratamento de dados pessoais que impossibilita a associação direta ou indireta de um indivíduo.

Exemplo: Para publicar os resultados de um estudo, o responsável utilizou métodos tecnológicos que não permitissem a identificação direta ou indireta de nenhum titular de dados.

Pseudonimização

É o tratamento que dificulta a identificação direta ou indireta de um indivíduo, por meio do uso de informação adicional mantida separadamente e em ambiente controlado e seguro.

Exemplo: Para fazer a pseudonimização dos dados, o pesquisador poderia criptografar os dados de modo a mascará-los. Considerando a guarda das “chaves”, o controlador pode “ligar e desligar” a conexão com o dado do titular.

Bases Legais

Para saber quando podemos tratar os dados, precisamos avaliar se há base legal e se o tratamento está de acordo com os princípios da LGPD.

As bases legais estão listadas no Art.7 da LGPD e não se sobrepõem entre si. São elas:

- Consentimento;
- Cumprimento de obrigação legal ou regulatória;
- Pela administração pública, para tratamentos necessários à execução de políticas públicas previstas em lei ou respaldadas em contratos, convênios, ou instrumentos congêneres,
- Para realização de estudos por órgãos de pesquisa;
- Para execução contratual ou procedimentos preliminares;
- Para exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da vida e da incolumidade física do titular ou terceiro;
- Tutela de saúde do titular;
- Legítimo Interesse;
- Proteção de crédito.

Bases Legais - exemplos

Cumprimento de obrigação legal ou regulatória

Empregador que manda os dados do empregado para o e-social.

Proteção de crédito

Banco de dados calcula o score de crédito de uma pessoa.

Execução contratual

Um titular de dados assina um contrato solicitando um cartão de crédito e seus dados serão processados pelo Banco e pela administradora, conforme contrato firmado.

Legítimo interesse

O Banco Santander compartilha dados de endereço de um titular em comum com uma de suas coligadas, para que ambos cadastros estejam atualizados e que o titular possa receber correspondências no endereço correto.

Consentimento

Compartilhamento de seus dados para ofertas de produtos e serviços diretamente por empresas parceiras.

ATENÇÃO: O consentimento do Titular significa a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Direitos dos Titulares

1. Confirmação da existência de tratamento

2. Acesso aos dados

3. Correção de dados incompletos, inexatos ou desatualizados

4. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos, ou tratados em desconformidade com o disposto nesta lei

5. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observando os segredos comercial e industrial

6. Eliminação dos dados pessoais tratador com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei

7. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados

8. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa

9. Revogação de consentimento, nos termos do §5º do art. 8º da Lei

Impactos e Consequências

Infringir a LGPD pode gerar consequências como: advertência, multa simples, multa diária, publicização da infração, bloqueio dos dados pessoais e eliminação dos dados pessoais a que se refere a infração (mais detalhes no art. 52 da LGPD).

ATENÇÃO: a sanção de publicidade da infração ou até mesmo uma investigação feita por ordem judicial ou administrativa pode gerar um grande impacto na confiança do cliente, então o risco reputacional é alto.

Como se adequar?

Para uma empresa se adequar à LGPD, ela precisará revisitar todos os seus processos e identificar quais deles é realizado o tratamento de dados pessoais, considerando sua empresa como um todo.

Sugestão de etapas para iniciar um programa de adequação:

Mapeamento: Através de um mapeamento exaustivo nas diferentes áreas da empresa, identificar onde estão os dados pessoais (sistemas, arquivos, banco de dados, etc.). Adicionalmente, importante entender o ciclo de vida do dado - onde é coletado, armazenado, utilizado, quem tem acesso, pra quem é transmitido e quando é descartado.

Base legal e princípios: Verifique se há base legal para realizar o tratamento dos dados identificados. Avalie se os princípios trazidos pela LGPD estão sendo contemplados nesses tratamentos de dados.

Riscos e políticas: Identifique os riscos envolvidos em seus processos e estabeleça controles para mitigá-los. Avalie eventuais deficiências e determine planos de ação para saná-las. Adicionalmente, revisite ou estabeleça novas políticas, procedimentos, controles de acesso, medidas de segurança, etc.

Prevenção e Revisão: proteja os dados por meio de medidas preventivas, tenha plano de gestão de incidentes e estabeleça um fluxo de monitoramento e revisão contínua.

Forma de pensar em dados

Privacy by Design

É a privacidade pensada desde a concepção de um produto ou serviço.

Exemplo: Ana usa um app que, desde a sua concepção, já foi pensado considerando a privacidade e a segurança dos dados pessoais a ele relacionados, garantindo o cumprimento dos aspectos legais de privacidade.

Privacy by Default

É a privacidade por padrão, ou seja, o mais restrito possível.

Exemplo: Ana usa o app e ao ser instalado pela primeira vez, veio com o modo de uso mais restrito possível. Ela tem que liberar o acesso para a coleta de mais informações nas funções que desejar utilizar.

Relatório de Impacto

O relatório de impacto à proteção de dados pessoais é definido como a *"documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco"*.

Dentro da empresa, uma vez identificados os tratamentos de dados pessoais mais críticos, há necessidade de elaborá-lo com detalhamento dos riscos relacionados a esse tratamento e as medidas aplicáveis para mitigação.

Orientações para cumprimento da LGPD

NUNCA divulgar a terceiros os dados pessoais que tenha acesso, salvo por autorização do Banco Santander;

MANTER controle de acesso aos dados pessoais visando sua confidencialidade;

GARANTIR que a finalidade quanto ao uso dos dados está sendo realizada de acordo com as diretrizes do Banco Santander;

Caso haja troca de dados com o Banco Santander ASSEGURAR que estão sendo compartilhados apenas dados necessários para atender a finalidade proposta.

Exemplos - bases legais

Consentimento – Pergunta feita ao cliente nos canais digitais, questionando se ele autoriza o compartilhamento de dados que forneceu ao Santander com terceiros.

Cumprimento de obrigação legal ou regulatória – Arquivamento de ligações de clientes feitas pela Central de Atendimento, por período determinado pelo Bacen.

Legítimo interesse – Prospecção, recrutamento e seleção de funcionários para o Banco, por meio do acesso ao banco de currículos.

Execução de Contrato – Coleta de dados pessoais para contratação de Seguro de Vida.

Exercício de direitos em processo – Acesso aos extratos de movimentação de conta para atuação em processos judiciais.

Proteção ao crédito – Acesso ao score do cliente para definição de limites de crédito disponíveis.

Exemplos - Princípios LGPD

Sabendo que o banco possui acesso a uma vasta base de dados pessoais de candidatos que cadastram seus currículos, alguns e-mails são disparados como teste com a oferta de produtos Santander para essas pessoas. – **O tratamento não esta em conformidade com os princípios de finalidade, adequação e necessidade, pois os dados foram obtidos para seleção de candidatos à vagas de emprego, um outro propósito.**

O banco disponibiliza ao titular a possibilidade de solicitar um dossiê contendo os dados que o Banco trata sobre ele. – **O tratamento está de acordo com a LGPD, pois todo o ecossistema Santander deve conceder acesso facilitado às informações que são tratadas garantindo o livre acesso.**

Ao acessar nossos canais digitais, a cliente é alertada com um opt-in, para dar o aceite aos Termos de Uso e Política de Privacidade do Banco. - **O tratamento está de acordo com a LGPD, pois todo cliente deve ser informado claramente sobre o uso de seus dados pessoais, por meio de políticas e/ou contratos para atender o princípio de transparência.**

Exemplos – Princípios LGPD

Um jovem estagiário fica surpreso com a quantidade de dados de clientes que consegue acessar e consulta quanto aquele famoso jogador de futebol tem em sua conta bancária para falar com seus amigos da faculdade. – **O tratamento não esta em conformidade com os princípios de segurança e prevenção, pois embora se tenha conhecimento deste tipo de informação, elas não devem ser compartilhadas e só podem ser acessadas para as finalidades corretas. Neste exemplo temos também o crime de quebra de sigilo bancário.**

Um funcionário sugere em uma reunião interna que a política de concessão de crédito utilize dados complementares para agregar a análise do perfil do cliente, tais como opinião política e biometria. – **O tratamento não está em conformidade com os princípios de não discriminação e necessidade, pois os dados de opinião política e biometria, são dados sensíveis e não podem ser utilizados para determinar ou não a concessão de um crédito.**