INTRODUÇÃO A LGPD?

O que é LGPD?

A LGPD (Lei Geral de Proteção de Dados) é uma lei brasileira que estabelece regras claras para a coleta, armazenamento, processamento e compartilhamento de dados pessoais de indivíduos. Ela foi inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês) da União Europeia e entrou em vigor em setembro de 2020.

O objetivo principal da LGPD é garantir a privacidade e a segurança dos dados pessoais dos cidadãos brasileiros, bem como garantir que as empresas que coletam e processam esses dados sejam responsáveis e transparentes em suas práticas.

A lei define dados pessoais como qualquer informação relacionada a uma pessoa física identificada ou identificável, como nome, endereço, número de identidade, endereço de e-mail, entre outros. A LGPD também estabelece direitos fundamentais aos titulares dos dados, como o direito de acesso, correção, exclusão e portabilidade dos dados pessoais.

A LGPD é aplicável a todas as empresas, organizações e instituições que coletam, armazenam ou processam dados pessoais de indivíduos no Brasil, independentemente do seu tamanho ou setor de atuação.

Consentimento

Na LGPD, o consentimento do titular dos dados é considerado elemento essencial para o tratamento, regra excepcionada nos casos previstos no art. 11, II, da Lei.

A lei traz várias garantias ao cidadão, como: poder solicitar que os seus dados pessoais sejam excluídos; revogar o consentimento; transferir dados para outro fornecedor de serviços, entre outras ações. O tratamento dos dados deve ser feito levando em conta alguns requisitos, como finalidade e necessidade, a serem previamente acertados e informados ao titular.

Quem fiscaliza?

Para fiscalizar e aplicar penalidades pelos descumprimentos da LGPD, o Brasil conta com a Autoridade Nacional de Proteção de Dados Pessoais, a ANPD. A instituição terá as tarefas de regular e de orientar, preventivamente, sobre como aplicar a lei. No entanto, não basta a ANPD (Lei nº 13.853/2019) e é por isso que a Lei Geral de Proteção de Dados Pessoais também prevê a existência dos agentes de tratamento de dados e estipula suas funções, nas organizações, como: o controlador, que toma as decisões sobre o tratamento; o operador, que realiza o tratamento, em nome do controlador; e o encarregado, que interage com os titulares dos dados pessoais e a autoridade nacional.

Com relação à administração de riscos e falhas, o responsável por gerir dados pessoais também deve redigir normas de governança; adotar medidas preventivas de segurança; replicar boas práticas e certificações existentes no mercado; elaborar planos de contingência; fazer auditorias; resolver incidentes com agilidade, com o aviso imediato sobre violações à ANPD e aos indivíduos afetados.

As falhas de segurança podem gerar multas de até 2% do faturamento anual da organização no Brasil – limitado a R$ 50 milhões por infração. A autoridade nacional fixará níveis de penalidade segundo a gravidade da falha e enviará alertas e orientações antes de aplicar sanções às organizações.

Objetivo

A Lei Geral de Proteção de Dados Pessoais (LGPD) vem para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A lei dispõe sobre o tratamento de dados feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Abrangência

Vale para: dados relacionados à pessoa (brasileira ou não) que esteja no Brasil, no momento da coleta; dados tratados dentro do território nacional, independentemente do meio

aplicado, do país-sede do operador ou do país onde se localizam os dados; dados usados para fornecimento de bens ou serviços.

Exceção

Não se aplica para fins exclusivamente: jornalísticos e artísticos; de segurança pública; de defesa nacional; de segurança do Estado; de investigação e repressão de infrações penais; particulares (ou seja, a lei só se aplica para pessoa física ou jurídica que gerencie bases com fins ditos econômicos). E não se aplica a dados de fora do Brasil e que não sejam objeto de transferência internacional.

Fundamentos e princípios

Fundamentos

- O tema proteção de dados pessoais, na LGPD, tem como fundamentos (art. 2º, LGPD):

- respeito à privacidade, ao assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada;

- a autodeterminação informativa, ao expressar o direito do cidadão ao controle, e assim, à proteção de seus dados pessoais e íntimos;

- a liberdade de expressão, de informação, de comunicação e de opinião, que são direitos previstos na Constituição brasileira;

- desenvolvimento econômico e tecnológico e a inovação, a partir da criação de um cenário de segurança jurídica em todo o país;

- a livre iniciativa, a livre concorrência e a defesa do consumidor, por meio de regras claras e válidas para todo o setor privado; e

- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas.

Princípios

A boa-fé no tratamento de dados pessoais é premissa básica. Além disso, é preciso refletir sobre questões como "Qual o objetivo deste tratamento?", "É preciso mesmo utilizar essa quantidade de dados?", "O cidadão com quem me relaciono deu o consentimento?", "O uso dos dados pode gerar alguma discriminação?". Essas são algumas das perguntas que devem ser feitas. Quer saber o que mais deve ser levado em conta na hora de tratar os dados? Confira então os princípios e as bases legais da Lei Geral de Proteção de Dados Pessoais.

Os seguintes princípios (art. 6º, LGPD) devem ser observados na hora de tratar dados pessoais:

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

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.

Direitos do titular

O que são dados pessoais? Segundo a LGPD

É simples. É considerado dado pessoal qualquer informação que permita identificar, direta ou indiretamente, uma pessoa que esteja viva, tais como: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies.

Glossário

Agentes de tratamento: o controlador e o operador

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

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

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável

Dado pessoal de criança e de adolescente: o Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou

político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

Garantia da segurança da informação: capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação

Garantia da segurança de dados: ver garantia da segurança da informação

Interoperabilidade: capacidade de sistemas e organizações operarem entre si. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, além dos padrões de interoperabilidade de governo eletrônico (ePING)

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico

Relatório de impacto à proteção de dados pessoais: 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

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

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro

Tratamento: toda operação realizada com dados pessoais; como as que se referem a:

acesso - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados

armazenamento - ação ou resultado de manter ou conservar em repositório um dado

arquivamento - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência

avaliação - ato ou efeito de calcular valor sobre um ou mais dados

classificação - maneira de ordenar os dados conforme algum critério estabelecido

coleta - recolhimento de dados com finalidade específica

comunicação - transmitir informações pertinentes a políticas de ação sobre os dados

controle - ação ou poder de regular, determinar ou monitorar as ações sobre o dado

difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados

distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido

eliminação - ato ou efeito de excluir ou destruir dado do repositório

extração - ato de copiar ou retirar dados do repositório em que se encontrava

modificação - ato ou efeito de alteração do dado

processamento - ato ou efeito de processar dados

produção - criação de bens e de serviços a partir do tratamento de dados

recepção - ato de receber os dados ao final da transmissão

reprodução - cópia de dado preexistente obtido por meio de qualquer processo

transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro

transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.

utilização - ato ou efeito do aproveitamento dos dados.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

A ISO 29100 e a LGPD

A ISO 29100 fornece uma estrutura de alto nível para a proteção de dados pessoais dentro de sistemas de informação, dispondo de aspectos técnicos, organizacionais e procedurais dentro desta estrutura, ajudando empresas a definir seus requisitos de privacidade a partir de um entendimento comum sobre proteção de dados privados dos titulares.

Como qualquer norma ISO sobre framework, ela está dividida nas seguintes partes e objetivos:

Escopo – Tem como objetivo estabelecer os limites e objetivos da 29100 que são: (i) estabelecer uma terminologia comum sobre privacidade, (ii) definir os atores e seus papéis no processamento de dados pessoais, descrever as considerações para proteção da privacidade, e fornecer as referências para os princípios de privacidade para tecnologia da informação.

Termos e definições – Foca em unificar os conceitos e estabelecer o entendimento comum de suas definições, fornecendo inclusive um anexo com as relações entre os conceitos da 27001 e 29100. Dentre estes conceitos, e claro como especialista em gestão de riscos, o conceito de privacy risk faz todo o sentido (inclusive alinhado com a ISO 31000).

Elementos básicos da estrutura de privacidade – Tem o objetivo de definir os componentes relacionados com processamento de dados privados, quais sejam: (i) atores papéis, (ii) interações, (iii) identificar dado pessoal, (iv) requisitos de proteção de dados, (v) política de privacidade, e (vi) controles de privacidade.

A título de exemplo, em atores e papéis foram definidos quatro tipos de que podem estar envolvidos no processamento de dados pessoais: (i) Titulares de DP, (ii) Controladores de DP , (iii) Operadores de DP (do inglês *PII processors*) e (iv) Terceiros (estes não processam dados a mando do controlador, podendo ser um controlador).

Interações – Apresenta os tipos de interações que podem ocorrer, apresentando uma tabela com os cenários destas interações entre os quatro tipos de atores definidos.

Identificação de Dados Pessoais – Tem o objetivo de apresentar orientações e clarificar como determinar se um dado é dado pessoal identificável (ou que pode identificar um titular), tocando em temas de características distintas e atributos que podem identificar titulares (p.ex. data de nascimento, nome, sexo, localização GPS, etc.).

Requisitos de proteção de privacidade – Tem o objetivo de fornecer uma visão geral dos diferentes fatores que podem influenciar os requisitos de proteção que são relevantes para uma empresa ou uma parte interessada no processamento de dados pessoais (DP).

Para os requisitos, a norma recomenda que a empresa deve executar periodicamente atividades de avaliação de riscos para entender os cenários de riscos no ambiente de TI que processa dados pessoais, sendo um possível produto o relatório de impacto à privacidade (ou do inglês *privacy impact assessment - PIA*). Este é um dos principais motivos pelos quais eu, como purista que sou em gestão de riscos, considero o PIA como uma avaliação de riscos.

Orienta também, e não poderia ser diferente, a adoção do processo de gestão de riscos definido na ISO 31000 – Escopo, Contexto e Critérios | Processo de avaliação de riscos | Tratamento de riscos | Comunicação e Consulta | Revisão e Análise Crítica | Registro e Relato.

Políticas de privacidade – Tem como objetivo de orientar o que deve ser considerado em uma política de privacidade, enaltecendo que a mesma deva referenciar tanto a política interna e externa.

Controles de privacidade – Tem como objetivo orientar como construir os controles de privacidade, sendo parte da abordagem geral de “Privacy by design” – devendo a conformidade com a privacidade ser considerada na fase de “design” do sistema que processa dado pessoal (DP) ao invés de ser “enxertado” depois.

Para esta norma, o processo de gestão de riscos é considerado como o método central para a definição de controles, sendo a sua identificação (controles) parte integrante da estrutura de gestão de segurança da informação da empresa.

Princípios de privacidade – Tem como objetivo apresentar os princípios de privacidade. Tais princípios foram extraídos dos principais princípios de diversos países e organizações internacionais. A estrutura definida na ISO 29100 procura orientar a aplicação destes princípios na TI das empresas, independente dos fatores sociais, culturais, legais e econômicos (mas que podem limitar a sua aplicação).

Em resumo, a norma ISO 29100, que é de 2011 (bem antiga), é fundamental para entendimento e adoção de linguagem comum para uma estrutura de privacidade para qualquer

empresa. Entendo que esta norma seja de leitura fundamental para as empresas que desejam implantar uma estrutura de privacidade para atendimento ao requisito regulatório.

Para atender requisitos regulatórios como a LGPD e GDPR que definem o que as empresas devem fazer, deve-se procurar melhores práticas que orientam como deve ser feito e esta norma é o ponto inicial de entendimento de como fazer.

ISO 27701 – Extensão ISO 27001/2 para Privacidade de Dados

A GDPR da UE (Regulamento Geral de Proteção de Dados) e a LGPD (Lei de Privacidade de dados brasileira) exigem que os controladores e processadores de dados pessoais implementem "medidas técnicas e organizacionais" apropriadas para protegê-lo, bem como medidas para garantir a privacidade dos dados pessoais.

No entanto, as regulamentações fornecem pouca orientação sobre a forma que essas medidas devem assumir.

Para resolver este problema a ISO (*International Organization for Standardization*) e a IEC (*International Electrotechnical Commission*) desenvolveram uma nova adição à família de normas de segurança da informação ISO 27000 para fornecer essa orientação: **ISO / IEC 27701 Técnicas de segurança – extensão à** ISO / IEC 27001 e ISO / IEC 27002 para gerenciamento de informações privadas **– Requisitos e diretrizes.**

O que é a ISO 27701?

O ISO.org diz que a ISO27701 *"especifica requisitos e fornece orientações para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gerenciamento de Informações de Privacidade (PIMS) na forma de uma extensão da ISO / IEC 27001 e ISO / IEC 27002 para gerenciamento de privacidade no contexto da organização. " …*

"especifica os requisitos relacionados ao PIMS e fornece orientações para controladores de PII e processadores de PII responsáveis e responsáveis pelo processamento de PII." …

“é aplicável a todos os tipos e tamanhos de organizações, incluindo empresas públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que são controladores de PII e / ou processadores de PII que processam PII dentro de um ISMS.”

De outra forma, a ISO 27701 especifica os requisitos e fornece orientações para estabelecer, implementar, manter e melhorar continuamente – um PIMS (*privacy information management system*) com base nos requisitos, objetivos e controles de controle na norma de gerenciamento de segurança da informação ISO 27001, e estendido por um conjunto de requisitos específicos da privacidade, objetivos e controles de controle.

A ISO 27001 estabelece os requisitos para um SGSI (sistema de gerenciamento de segurança da informação, do inglês ISMS), uma abordagem baseada em riscos que abrange pessoas, processos e tecnologia. A certificação credenciada de forma independente para a ISO 27001 fornece às partes interessadas a garantia de que os dados estão sendo adequadamente protegidos.

“As organizações podem implementar a ISO 27001 e a ISO 27701 juntas como um único projeto de implementação”

As organizações que implementaram a ISO 27001 poderão usar a ISO 27701 para estender seus esforços de segurança para cobrir o gerenciamento de privacidade – incluindo o processamento de dados pessoais / PII (informações de identificação pessoal) – que os ajudarão a demonstrar conformidade com as leis de proteção de dados, como o GDPR.

As organizações podem implementar a ISO 27001 e a ISO 27701 juntas como um único projeto de implementação. Como a ISO 27701 simplesmente expande os requisitos e orientações fornecidos pela ISO 27001 e seu código de prática, a ISO 27002, não há necessidade de combinar dois sistemas de gerenciamento ou projetos de implementação separados.

Qual é a diferença entre um sistema de gerenciamento de informações privadas e um sistema de gerenciamento de informações pessoais?

Enquanto a ISO 27701 estabelece os requisitos para um sistema de gerenciamento de informações privadas, a BS-10012 é o padrão britânico para um sistema de gerenciamento de informações pessoais (*Personal Information Management System*).

Na realidade não há diferença material entre os dois termos – ambos são sistemas de gerenciamento projetados para proteger informações pessoais – e, para o bem das atividades diárias, você pode assumir o acrônimo 'PIMS' para se referir a ambos. No entanto, segundo o IT Governance existem algumas diferenças notáveis entre as duas abordagens, que apresentamos abaixo.

GDPR	ISO 27701
Personal data	PII
Data controller	PII controller
Data processor	PII processor
Data subject	PII principal
Data protection by design	Privacy by design
Data protection by default	Privacy by default

IT Governace GDPR x ISO27701

Mapeamentos de controle ISO 27701

Além de fornecer requisitos, controles e objetivos específicos de privacidade para controladores e processadores, a ISO 27701 inclui anexos que os mapeiam para:

ISO 29100 *(Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade)* ;

ISO 29151 *(Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de informações de identificação pessoal)* ; e

ISO 27018 *(Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII)* .

Ele também contém um anexo que mapeia seus requisitos e controles com os requisitos do GDPR; portanto, a ISO 27701 pode ser usada como um guia de conformidade do GDPR e LGPD por controladores e processadores de dados.

Por exemplo, as obrigações dos controladores de dados de atender aos direitos dos titulares de dados de acordo com o GDPR/LGPD são cobertas pelos controles da ISO 27701, que cobrem as obrigações para com os diretores de PII e também são fornecidas orientações para a implementação de cada controle.

Demonstrar conformidade com GDPR com ISO 27701 e ISO 27001

A implementação das normas ISO 27701 e ISO 27001 permitirá que você atenda aos requisitos de privacidade e segurança da informação do GDPR, LGPD e de outros regimes de proteção de dados e demonstre que possui acordos de gerenciamento para “medidas técnicas e organizacionais apropriadas” para proteger os dados pessoais que você processa e defender os direitos dos titulares dos dados, em conformidade com o princípio da responsabilidade do regulamento (artigo 5.º, n.º 2).

Os artigos da GDPR e LGPD que discutem mecanismos de certificação de proteção de dados e selos e marcas de proteção de dados. Ainda não existem tais mecanismos. No entanto, é possível obter certificação credenciada de forma independente para a ISO 27001 – e, por extensão, ISO 27701 se você implementar seus controles – o que demonstrará às partes interessadas e reguladores que sua organização está seguindo as melhores práticas internacionais quando se trata de proteger dados pessoais / PII.