Workbook
Privacidade, Dados Pessoais e LGPD

Edição 202101

Sobre o autor

Original em inglês (base GDPR):

Leo Besemer
CertiQA
https://www.certiqa.nl/website/
Contato: leo.besemer@certiqa.nl

Adaptação em português (base LGPD)

Daniela Cabella
Primeira certificada como DPO pelo EXIN no continente americano
https://www.linkedin.com/in/danielacabella/

Gisele Kauer
Advogada certificada pelo EXIN (PDPE e ISFS)
https://www.linkedin.com/in/giselekauer

Conteúdo

EXIN Privacy & Data Protection Essentials

Introdução

Este workbook apresenta um resumo da literatura para os candidatos que estudam para o exame EXIN Privacy & Data Protection Essentials em português – base LGPD (PDPE). Para os requisitos mais recentes para o exame, consulte o Guia Oficial de Preparação do EXIN, que pode ser baixado em www.exin.com.

Em uma era digital, as informações sobre as pessoas estão se tornando cada vez mais valiosas. Facilitadas por novas tecnologias, as organizações coletam e armazenam dados em grande escala. Esta recente explosão de dados apresenta desafios específicos de segurança, especialmente quando se trata de dados pessoais, devido à regulamentação rigorosa em relação à proteção de dados.

Privacidade e proteção de dados pessoais devem ser uma prioridade para qualquer organização.

Organizações que processam dados pessoais de pessoas localizadas no território brasileiro devem cumprir a Lei Geral de Proteção de Dados Pessoais (LGPD). As organizações localizadas fora do Brasil também deverão observar a LGPD ao oferecer produtos e/ou serviços a pessoas físicas no Brasil ou realizar qualquer tipo de tratamento no país. A adesão à LGPD previne multas e aumenta a confiança dos clientes.

Ter profissionais certificados com o nível certo de conhecimento pode ajudar a preparar uma organização para cumprir a LGPD e melhorar o nível de conformidade com a legislação. O programa EXIN Privacy & Data Protection Essentials (PDPE) traz a base para o cumprimento da LGPD.

EXIN, janeiro de 2021.

Fundamentos de Privacidade

1 Definições e Contexto Histórico

Neste capítulo, veremos a história da privacidade e proteção de dados e a relação entre os dois conceitos. Com isso, analisaremos algumas definições básicas, já que elas são usadas na Lei Geral de Proteção de Dados (LGPD). Alguns dos termos e conceitos são explicitamente definidos no Artigo 5º da LGPD e outros são derivados do direito internacional.

1.1 A História das Regulações de Proteção de Dados

As recentes invenções e métodos de negócios chamam a atenção para o próximo passo que deve ser tomado para a proteção da pessoa e para assegurar ao indivíduo... o direito de "estar sozinho"...Vários dispositivos mecânicos ameaçam cumprir a previsão de que "o que é sussurrado no armário deve ser proclamado a partir dos telhados ".

Fonte: https://www.brandeis.edu/now/2013/july/privacy.html (acessado em 18 de março de 2017)

Enquanto alguém poderia pensar que este texto foi escrito recentemente, Louis D. Brandeis o escreveu em um artigo na revista Harvard Law Review, em 1890. Este direito de não ser incomodado ou sofrer invasões, acabou se tornando a base sobre a qual o Artigo 12 da Declaração Universal dos Direitos Humanos (DUDH), publicada em 1948.

Ninguém estará sujeito a interferências arbitrárias em sua privacidade, família, lar ou correspondência, nem a ataques à sua honra e reputação. Todos têm o direito de proteção da lei contra tais interferências ou ataques.

Fonte: https://www.un.org/en/universal-declaration-human-rights/ (acessado em 18 de março de 2017)

O rápido progresso no processamento de dados e o aumento das possibilidades no uso de telecomunicações na década de 1970 coincidiram com o desenvolvimento da União Europeia, que aumentou o comércio transfronteiriço. Como resultado, sentiu-se a necessidade de novos padrões que permitissem aos indivíduos exercer controle sobre suas informações pessoais. Ao mesmo tempo, o comércio internacional precisava de um fluxo internacional de informações livre. O desafio é encontrar um equilíbrio entre as preocupações com a proteção das liberdades pessoais e a possibilidade de apoiar o livre comércio em toda a Europa.

Os Estados-Membros da União Europeia assinaram na Convenção Europeia de Direitos Humanos (ECHR - European Convention of Human Rights, 1950) um tratado para defender os direitos humanos em toda a União Europeia, entre eles **o direito ao respeito pela vida privada e familiar**.

Um primeiro esforço para consolidar a **proteção da privacidade** e a **necessidade de fluxo internacional de dados pessoais livre** veio da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em 1980: Diretrizes para a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais (*Guidelines on the Protection of Privacy and Trans-border flows of Personal Data)*. Essas diretrizes foram formalizadas em 1981 pela Convenção para a Proteção de Indivíduos no que diz respeito ao Processamento Automático de Dados Pessoais, também conhecido como Tratado de Estrasburgo.

Quando o desenvolvimento do comércio internacional e a necessidade de proteção aumentaram, sentiu-se a necessidade de harmonização da legislação europeia sobre privacidade. Isso resultou, em 1995, na "Diretiva de Proteção de Dados" n. 95/46/EC.

A Carta dos Direitos Fundamentais da União Europeia (a 'Carta', proclamada em dezembro de 2002) incluía os princípios gerais estabelecidos na CEDH. A Carta refere-se explicitamente à proteção da privacidade e à proteção de dados pessoais como um **direito** fundamental:

Artigo 7: Respeito à vida privada e familiar
1. Toda pessoa tem o direito à sua vida privada e familiar, sua casa e sua correspondência.

Artigo 8: Proteção de dados pessoais
1. Toda pessoa tem direito à proteção dos dados pessoais que lhe digam respeito.
2. Esses dados devem ser tratados de forma justa para fins específicos e com base no consentimento da pessoa em causa ou em qualquer outra base legítima estabelecida por lei. Todos têm o direito de acessar os dados coletados sobre ele e o direito de retificá-los.
3. O cumprimento destas regras está sujeito ao controle de uma autoridade independente.

Fonte: Carta dos Direitos Fundamentais da União Europeia.

Enquanto o progresso no processamento de dados aumentava a cada ano, o comércio internacional era dificultado por leis diferentes. As regras e regulamentos nos Estados-Membros, embora baseados na Diretiva n. 95/46/CE, ainda eram bastante diversas. Após anos de discussão, o Regulamento n. 2016/679, o *General Data Protection Regulation* (GDPR), foi publicado em 25 de maio de 2016. O GDPR, aplicável de forma imediata e como lei em todos os países da Área Econômica Europeia (AEE), entrou em vigor em 25 de maio de 2018. O Regulamento revoga a Diretiva n. 95/46/CE. Isso significa que todas as leis nacionais baseadas nessa Diretiva devem ser adaptadas ao GDPR. Nos termos do artigo 94(2) do GDPR, as referências à Diretiva revogada devem entender-se como sendo feitas ao novo Regulamento[1].

No Brasil, o tema de privacidade e proteção de dados, que já era discutido, ganhou força com a chegada do GDPR, uma vez que o Regulamento europeu poderia se tornar uma barreira comercial entre os Estados-Membros da Área Econômica Europeia (AEE) e as empresas situadas em países sem legislação adequada sobre a matéria.

As bases para a legislação nacional específica de proteção de dados foram construídas, principalmente por meio da consolidação do direito à privacidade como um direito fundamental na Constituição Federal de 1988, como um direito da personalidade no Código Civil de 2002, como um direito assegurado até mesmo pela Lei de Acesso à Informação (2011), como princípio e direito estabelecidos pelo Marco Civil da Internet (2014), com o estabelecimento de padrões de segurança definidos pelo Decreto nº 8.771 (2016) para o tratamento de dados pela internet.

Em agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018, mais conhecida como “LGPD”), foi aprovada. Essa lei específica e unificada sobre proteção de dados pessoais coloca o Brasil e as organizações estabelecidas em território nacional em outro patamar no cenário econômico mundial, com um maior nível de confiança por parte do mercado, da comunidade internacional e maior protagonismo na economia digital.

[1] Regulação versus Diretiva: ao contrário de uma diretiva que deve ser assimilada dentro da legislação nacional de cada Estado-Membro, uma Regulação é vinculante e diretamente aplicável a todos os Estados-Membros. O GDPR é "Texto com Relevância EEE", o que significa que se aplica a todos os países do Espaço Econômico Europeu (EEE) ou da Área Econômica Europeia (AEE), composto por todos os Estados-Membros da UE, Islândia, Liechtenstein e Noruega.

A conformidade com a LGPD não apenas evita multas e outras sanções, mas agrega valor e uma série de benefícios operacionais à organização[2].

1.1.1 Cronologia da Proteção de Dados

Ano	Nome	Sigla
1948	Declaração Universal dos Direitos Humanos	DUDH (UHDR)
1950	Convenção Europeia sobre Direitos Humanos	CEDH (ECHR)
1981	Convenção para Proteção de Indivíduos relativamente ao Processamento Automático de Dados Pessoais	ETS 108 = EU Tratado de Estrasburgo
1988	Constituição Federal	CF
1995	Diretiva n. 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados	Diretiva de Privacidade (válida até 25/5/2018)
2002	Carta dos Direitos Fundamentais da União Europeia Código Civil	CEDH (EU Charter) CC
2011	Lei de Acesso à Informação	LAI
2014	Marco Civil da Internet	MCI
2016	Regulamento Geral de Proteção de Dados (EU - 2016/679) Decreto nº 8.771/2016	'GDPR' (a partir de 25/5/2018) Decreto nº 8.771/2016
2018	Brasil: Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018)	LGPD

1.2 Escopo material e territorial da LGPD

1.2.1 Escopo material

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 1º, caput)

A LGPD se aplica a dados pessoais apresentados de forma estruturada ou não, desde sistemas de banco de dados totalmente automatizados até arquivos baseados em papel, como os prontuários médicos clássicos ainda usados em algumas clínicas médicas.

Existem algumas exceções. A LGPD não se aplica ao tratamento de dados pessoais de cunho puramente doméstico, ou seja, realizado para fins exclusivamente particulares e não econômicos. Também não se aplica ao tratamento feito para cumprir finalidades unicamente jornalísticas e artísticas.

O tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais será objeto de legislação específica, e a Autoridade Nacional de Proteção de Dados (ANPD) emitirá opiniões técnicas ou recomendações referentes a esses temas e deverá solicitar Relatórios de Impacto à Proteção de Dados (RIPD) aos respectivos responsáveis.

[2] Conforme dados do Relatório "Da Privacidade ao Lucro: como obter retornos positivos sobre investimento em privacidade", publicado pela Cisco em 2020. Fonte: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/2020-data-privacy-report-ptbr.pdf. Acesso em 23.12.2020.

Por fim, não se aplica a LGPD ao tratamento de dados pessoais que não ocorra, de nenhuma forma, em território brasileiro e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados que envolva o Brasil.

1.2.2 Escopo territorial

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- I - a operação de tratamento seja realizada no território nacional;
- II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
- III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709/2018 (art. 3º, caput e § 1º).

Qualquer tratamento de dados pessoais no contexto das atividades de um estabelecimento de um controlador ou de um operador no Brasil deve ser efetuado em conformidade com a LGPD, independentemente do local (no mundo) em que os dados sejam tratados efetivamente (ex: controlador tem sede no Brasil, mas os dados estão em um servidor de *cloud computing* no Arizona, EUA).

A LGPD também se aplica ao tratamento relacionado ao comércio ("a oferta ou o fornecimento de bens ou serviços") e ao tratamento de dados pessoais de pessoas que estão localizadas no território nacional. Isso tem consequências de longo alcance. Por exemplo o caso de uma empresa canadense que trata dados pessoais de um cidadão argentino para uma compra online. Se esse cidadão argentino estiver visitando João Pessoa (Brasil) no momento da compra e a empresa canadense estiver oferecendo bens ou serviços para o Brasil de forma intencional (porque eles enviam produtos para o Brasil e apresentam uma versão da Política de Privacidade em português do Brasil, por exemplo), esse tratamento está sujeito à LGPD.

Além disso, a LGPD se aplica ao tratamento de dados pessoais por um controlador não estabelecido em território brasileiro, mas em que “os dados objeto do tratamento tenham sido coletados em território nacional” (art. 3º, III, LGPD).

1.3 Definições

Nos primeiros itens da LGPD, a disciplina da proteção de dados pessoais está explicitamente ligada à Constituição Federal.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709/2018 (art. 2º)

Nesse sentido, a proteção de dados pessoais é um meio efetivo para garantir o pleno exercício de direitos e liberdades fundamentais das pessoas - dentre eles, a sua privacidade.

1.3.1 Privacidade

A privacidade é definida como o direito a respeitar a vida privada (particular, íntima) e familiar de uma pessoa, sua casa e suas comunicações.

1.3.2 Proteção de Dados

É importante destacar que a LGPD não protege todo e qualquer tipo de dado, mas somente os dados definidos no art. 5º como “pessoais”. Dados exclusivamente relacionados a estratégias de negócios ou planejamento de novos produtos, por exemplo, podem ser considerados “sigilosos” ou “confidenciais” e devem ser protegidos de acessos indevidos ou não autorizados, mas não são regulados pela LGPD.

1.3.3 Dados Pessoais

O art. 5, inciso I, da LGPD define dados pessoais como:

Art. 5º Para os fins desta Lei, considera-se:

- I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709/2018 (art. 5, inciso I)

Dados pessoal significa qualquer informação relativa a uma pessoa natural identificada ou identificável (titular dos dados). Uma pessoa natural identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos de identidade física, fisiológica, identidade genética, mental, econômica, cultural ou social daquela pessoa natural.

Qualquer informação pode ser tomada literalmente. Inclui informações objetivas, como atributos que podem ser medidos - por exemplo, tipo sanguíneo, tamanho do sapato ou a quantidade de álcool no sangue da pessoa. Também inclui informações subjetivas, tais como opiniões sobre uma pessoa (por exemplo, Ana é uma boa economista). Para que as informações sejam "dados pessoais", elas não precisam ser verdadeiras ou comprovadas. Mentiras ou dados incorretos sobre uma pessoa ainda podem ser considerados dados pessoais.

O conceito de dados pessoais não se limita a informações que possam ser consideradas prejudiciais à vida privada e familiar do indivíduo. O meio em que as informações estão contidas também é irrelevante. O conceito de dados pessoais inclui informações disponíveis em qualquer forma: texto, figuras, gráficos, fotografias, vídeo, áudio ou qualquer outra forma possível.

1.3.4 Pessoa Natural

Juridicamente, uma pessoa natural é um ser humano, um indivíduo capaz de assumir obrigações e de ter direitos. Portanto, a princípio, a LGPD não se aplica a pessoas falecidas. Nesse caso, falamos do direito à honra e institutos presentes no Código Civil brasileiro.

1.3.5 Dados pessoais diretos, indiretos e pseudonimizados

Na prática, há três tipos de dados pessoais.

1.3.5.1 Dados pessoais diretos

Dados pessoais diretos são dados que podem ser atribuídos diretamente a um indivíduo específico sem o uso de informações adicionais. Por exemplo, a foto do indivíduo, seu DNA, impressão digital. Os nomes podem ser dados pessoais diretos se forem muito raros, mas a maioria dos nomes não é considerada exclusiva e, portanto, não são dados pessoais diretos. Um título único, como "o atual ministro da economia do Brasil", também é uma referência direta a um indivíduo, ou seja, dados pessoais diretos.

1.3.5.2 Dados pessoais indiretos

Os dados pessoais indiretos são dados que podem estar ou poderão estar no futuro vinculados a um indivíduo específico usando informações adicionais. Por exemplo, a placa numérica de um carro é um dado pessoal indireto, porque é possível rastrear o carro até seu proprietário usando informações adicionais (neste caso, as informações em um banco de dados eram as placas de matrícula relacionadas aos proprietários dos carros). O mesmo é válido para números exclusivos atribuídos a pessoas pelo governo (número de previdência social) ou por um provedor de serviços internet (endereço IP). O fato de nem todos os controladores poderem rastrear uma placa de carro, número de segurança social ou endereço IP associado a um indivíduo não é importante. O fato de que isso seja possível faz com que sejam dados pessoais indiretos.

Os nomes mais comuns são dados pessoais indiretos, pois não apontam para uma pessoa específica. Para distinguir um determinado "João da Silva" de outros indivíduos com esse mesmo nome são necessárias informações adicionais, como o endereço de residência e data de nascimento, por exemplo.

1.3.5.3 Dados pessoais pseudonimizados

Pseudonimização de dados é o processo de disfarçar identidades. O objetivo desse processo é ser capaz de coletar dados adicionais relacionados ao mesmo indivíduo sem precisar conhecer sua identidade. Um exemplo pode ser uma câmera registrando quantos carros únicos passam por uma ponte em uma estrada. O número da placa é um dado pessoal indireto. O controlador substituiria cada número da placa por uma chave ou pseudônimo exclusivo, mantendo uma tabela separada vinculando cada chave à placa correspondente. O controlador pode enviar esses dados pseudonimizados para um operador, mantendo a chave em um local seguro.

Dados pseudonimizados são um tipo de dados pessoais indiretos, onde os dados adicionais necessários para identificar os titulares dos dados ('a chave') estão disponíveis apenas para o controlador. O processo é reversível desde que a chave exista. Consequentemente, dados pseudonimizados de uma pessoa são considerados dados pessoais, porque a identificação ainda é tecnicamente possível.

Já a anonimização é o processo pelo qual as informações deixam de ter quaisquer vínculos diretos e indiretos às pessoas naturais a quem se relacionavam originalmente. Dados

anonimizados, portanto, **não são mais** considerados dados pessoais e a LGPD não se aplica a eles (pois a lei se aplica somente a dados pessoais). Dados pseudonimizados podem ser anonimizados com a destruição (sem volta) da chave.

Por exemplo, para pesquisas sobre saúde e hábitos alimentares, é chamado um grupo selecionado de titulares de dados. Os nomes, números de telefone e outros dados de identificação dos titulares dos dados são conhecidos e mantidos em um banco de dados, para o qual os titulares dos dados deram sua permissão. Os titulares dos dados são chamados várias vezes durante a pesquisa. Depois que o período da pesquisa termina, todos os dados identificáveis são apagados. Isso significa que os dados não podem mais ser vinculados aos titulares de dados específicos, porque não existe uma chave. Somente dados pessoais mais gerais, como sexo e categoria etária, estão vinculados aos dados sobre saúde e hábitos alimentares. Em outras palavras, os dados estatísticos que resultaram da pesquisa são anonimizados.

1.3.5.4 Dados pessoais sensíveis

A LGPD distingue várias categorias de dados pessoais que necessitam um tratamento especial. As categorias de dados pessoais sensíveis são:

- dados que revelam origem racial ou étnica
- dados que revelam opiniões políticas
- dados que revelam crenças religiosas
- dados que revelam convicções filosóficas
- dados que revelam filiação sindical
- dados genéticos
- dados biométricos
- dados relativos à saúde
- dados relativos à vida sexual ou orientação sexual de uma pessoa natural

Os dado pessoais sensíveis somente podem ser tratados dentro das hipóteses do art. 11 da LGPD.

1.3.6 Tratamento

No que diz respeito à LGPD, a definição de tratamento é ampla, exemplificativa e aplicável somente a operações com dados pessoais (e não de quaisquer tipos de dados):

> Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
>
> Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 5, inciso X)

Na verdade, é difícil pensar em algo que possa ser feito com dados pessoais, mas não estaria contido na definição.

A coleta de dados pessoais é tratamento. O armazenamento de dados pessoais é tratamento. Destruir dados pessoais também é tratamento. Mesmo fazer um backup de um servidor que não é seu, mas contém dados pessoais, seria considerado um tipo de armazenamento, incluído na definição de tratamento.

1.4 Papéis, Responsabilidade e Partes Interessadas (stakeholders)

1.4.1 Controlador

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

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 5, inciso VI)

O controlador é a pessoa natural ou jurídica responsável pela **determinação das finalidades e meios do tratamento dos dados pessoais**.

É responsabilidade e o papel do controlador implementar medidas técnicas e organizacionais apropriadas para cumprir a LGPD, incluindo políticas apropriadas de proteção de dados. Além disso, o controlador deve ser capaz de demonstrar que o processamento é executado de acordo com a LGPD.

1.4.2 Operador

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

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 5, inciso VII)

Um operador sempre age 'em nome do controlador' e deve cumprir as instruções do controlador. O meio mais adequado para definir as instruções do controlador para o operador é contrato firmado entre eles.

1.4.3 Encarregado pelo Tratamento dos Dados Pessoais ou Data Protection Officer (DPO)

De acordo com a definição de “encarregado” pela LGPD, controladores e operadores devem nomear um Data Protection Officer (DPO). O DPO é uma pessoa que tem a tarefa formal de centralizar toda a comunicação sobre proteção de dados pessoais, garantir que a organização esteja ciente de suas responsabilidades e obrigações de proteção de dados e envidar esforços para que sejam cumpridas, sugerindo medidas técnicas e administrativas (que poderão ser acatadas ou não pelo agente de tratamento) para atendimento à LGPD e demais normas incidentes sobre a matéria.

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);

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 5º, inciso VIII)

A princípio, todos os agentes de tratamento devem indicar um DPO, mas a autoridade nacional poderá definir exceções a essa obrigatoriedade. De todo o modo, sendo nomeado, a organização deverá publicar os detalhes de contato e identificação do DPO, para que os titulares de dados e a autoridade nacional possam chegar ao DPO.

Em analogia ao artigo 38 do GDPR, o controlador e o operador devem garantir que o DPO seja envolvido, de forma adequada e em tempo hábil, em todas as questões relacionadas à proteção de dados pessoais. Os agentes de tratamento têm a obrigação de apoiar o DPO no desempenho de suas tarefas, fornecendo recursos necessários para realizar essas tarefas e acesso aos dados pessoais e operações de tratamento, e manter seu conhecimento especializado.

Além disso, o DPO deve reportar à alta gestão, garantindo uma **posição independente**, e sua autonomia deve ser protegida, assim como previsto pelo GDPR:

O controlador e o processador devem assegurar que o DPO não receba instruções sobre o exercício dessas tarefas. Ele não deve ser dispensado ou penalizado pelo controlador ou pelo processador por executar suas tarefas. O DPO deve reportar diretamente ao mais alto nível de gerenciamento do controlador ou do processador.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 38 (3)

1.4.3.1 Tarefas do Encarregado (DPO)

O Encarregado (DPO) deve ter pelo menos as seguintes tarefas:

- I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- II - receber comunicações da autoridade nacional e adotar providências;
- III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

a) A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 41, §§ 2º e 3º)

Além dessas atividades, o encarregado (DPO) também deve, em analogia ao artigo 39 (1) do GDPR, informar e aconselhar o controlador ou o operador e os empregados que efetuam o tratamento, monitorar a conformidade com a legislação de proteção de dados e com as políticas do controlador ou dos operadores no tocante à proteção dos dados pessoais, e prestar aconselhamento no que diz respeito à elaboração do relatório de impacto à proteção de dados.

2 Tratamento de Dados Pessoais

Qualquer operação com dados pessoais está contida na definição de tratamento. O art. 6 da LGPD detalha os princípios do tratamento de dados.

2.1 Princípios de Tratamento de Dados

O tratamento de dados pessoais precisa sempre estar em conformidade com os princípios elencados na LGPD. Esses princípios são:

- Finalidade
- Adequação
- Necessidade
- Livre acesso
- Qualidade dos dados
- Transparência
- Segurança
- Prevenção
- Não discriminação
- Responsabilização e prestação de contas

2.1.1 Finalidade

Os dados pessoais devem ser tratados para cumprir propósitos legítimos, autorizados por lei, específicos, explícitos e informados ao titular.

A regra geral é que não devem ser objeto de tratamento posterior incompatível com essas finalidades originais; no entanto, o § 7º do art. 7º da LGPD permite que os dados de acesso público ou tornados manifestamente públicos pelo próprio titular sejam tratados para novas finalidades, desde que: (i) sejam observados os propósitos legítimos e específicos para o novo tratamento, (ii) sejam garantidos meios efetivos para que os titulares possam exercer plenamente seus direitos, e (iii) sejam cumpridos os fundamentos e os princípios da LGPD.

2.1.2 Adequação

Considerando-se o contexto do tratamento, os dados pessoais devem ser tratados de forma compatível com as finalidades informadas ao titular. Esse princípio tem por objetivo garantir a ciência do titular sobre o que é feito com seus dados, bem como possibilitar certo controle e o efetivo exercício de seus direitos, quando aplicável.

Para o cumprimento desse princípio, é importante garantir que a ciência seja dada ao titular em tempo hábil; ou seja, caso um tratamento já tenha sido finalizado e a ciência tenha sido dada posteriormente, como seria possível o titular exercer seu direito de oposição (art. 18, § 2º, LGPD), quando cabível? O exercício desse direito certamente estaria prejudicado.

Vale ressaltar que a aplicação desse princípio, assim como dos demais, deve ser considerada a partir da entrada em vigor da LGPD.

2.1.3 Necessidade

Os dados pessoais devem ser pertinentes, proporcionais e não excessivos, isto é, **limitados ao mínimo necessário** em relação aos fins para os quais são tratados. Deve-se levar em consideração não apenas os tipos (categorias) de dados pessoais necessários para cumprir as finalidades do tratamento, mas também o volume de dados, se não é possível atender ao mesmo objetivo do tratamento de forma subsidiária, menos invasiva à privacidade, e o período necessário para o cumprimento das finalidades legítimas.

Por exemplo, não é necessário ter permissão de acesso às fotos salvas em um dispositivo móvel para permitir que um usuário jogue um jogo online de "paciência" ou "campo minado". Também não é necessário coletar as intenções de votos de todos os brasileiros para se ter uma ideia da tendência relacionada ao resultado das eleições – basta coletar uma porcentagem proporcional à população de cada estado da federação e do distrito federal.

Ainda, caso se deseje saber apenas uma média de quantas pessoas passam por determinada estação de metrô por dia, não é necessário coletar e registrar seus dados pessoais de nenhuma forma – basta contabilizar o número de acessos ao metrô (entradas/saídas) que a catraca registra, de forma anônima, por dia.

Finalmente, caso determinados dados pessoais sejam coletados única e exclusivamente para fins de cumprimento de obrigação legal, por exemplo, eles devem ser eliminados, de forma segura (sem possibilidade de recuperação), após atingido esse propósito.

Podemos dizer, portanto, que a definição do princípio da necessidade, de forma ampla, abrange os princípios da necessidade de forma estrita (menor número de tipos ou categorias de dados pessoais possível), proporcionalidade (menor volume de dados pessoais possível), subsidiariedade (busca do meio menos invasivo à privacidade possível) e temporalidade (tratamento pelo tempo mínimo possível necessário para o cumprimento das finalidades legítimas).

2.1.4 Livre Acesso

Os agentes de tratamento devem garantir aos titulares de dados pessoais meios eficazes para que possam realizar consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Essas informações podem ser colocadas nas políticas de privacidade dos sites e aplicações, por exemplo, podendo haver também uma área logada (quando aplicável) e/ou um canal de comunicação para que maiores detalhes sobre essas informações possam ser obtidos.

2.1.5 Qualidade dos Dados

Os dados pessoais devem ser precisos (exatos), claros, relevantes e atualizados, e todas as medidas razoáveis devem ser tomadas para garantir que eventuais dados incorretos, inexatos, obscuros ou desatualizados sejam retificados.

O atendimento a esse princípio depende da participação tanto do titular de dados como do próprio agente de tratamento. O titular é responsável por verificar seus dados pessoais e corrigi-los ou atualizá-los, sempre que aplicável, e o agente de tratamento também deve, do seu lado, buscar garantir que o titular de dados tenha meios para acessar e atualizar ou retificar seus dados. Também poderá utilizar dados públicos ou tornados manifestamente públicos pelo próprio titular de dados para corrigir ou atualizar essas informações, respeitados os preceitos da LGPD.1

2.1.6 Transparência

Os titulares devem ter fácil acesso a informações clara e precisas sobre o tratamento de seus dados pessoais e saber quais são os agentes envolvidos. O nível de detalhamento das informações deve respeitar os segredos comerciais e industriais. Isso significa, por exemplo, mencionar em uma política de privacidade quais categorias de dados (como faixa etária, renda, imóveis em nome próprio) serão levadas em consideração para o estudo da concessão ou não de crédito, mas a forma de valorar e equacionar cada dado é segredo comercial e não deverá ser revelada.

2.1.7 Segurança

Os agentes de tratamento devem aplicar medidas técnicas e administrativas para garantir a segurança adequada dos dados pessoais contra quaisquer tipos de tratamentos não autorizados, sejam eles acidentais ou ilícitos. Medidas como treinamento em segurança da informação para os funcionários envolvidos no tratamento, de modo a minimizar falhas humanas, controle de acesso, plano de resposta a incidente testado e implementado com sucesso, criptografia nos dados em trânsito e em repouso, backup, política de segurança da informação completa, atualizada, amplamente divulgada entre os colaboradores e com forte adesão ao seu conteúdo são alguns exemplos que cumprem o princípio da segurança.

Vale ressaltar que as medidas devem levar em consideração os dados pessoais tanto em meio eletrônico como físico (em papel, por exemplo). Recomenda-se seguir o framework da ISO 27001 para implementar controles eficazes de segurança da informação.

2.1.8 Prevenção

Esse princípio está contido dentro do princípio da segurança, mas a LGPD acabou por dar destaque à prevenção de forma proposital, demonstrando a importância em procurar evitar ao máximo que incidentes com dados pessoais ocorram. Além das medidas de detecção e resposta a incidentes, também é necessário adotar medidas técnicas e administrativas para prevenir que eventuais incidentes ocorram.

2.1.9 Não Discriminação

É expressamente proibido qualquer tipo de tratamento de dados pessoais que implique discriminação “ilícita” ou “abusiva”. A LGPD utiliza esses dois termos específicos porque a discriminação no sentido amplo de “distinção” ou “classificação” lícita e não abusiva é permitida. Exemplo: a segmentação de audiência para fins de envio de publicidade direcionada. É permitido classificar públicos-alvo para enviar comunicações relacionadas a temas, interesses, faixas etárias ou perfis de consumo de modo a facilitar que o titular de dados acesse mais ofertas que possivelmente lhe interessem e deixe de receber comunicações sobre assuntos, produtos e/ou serviços pelos quais não tem interesse algum.

2.1.10 Responsabilização e Prestação de Contas

Os agentes de tratamento devem ser capazes de demonstrar, com provas objetivas e eficazes, o cumprimento da legislação de proteção de dados pessoais e o quão eficazes são as medidas técnicas e administrativas que adotou. Por isso, a documentação e o registro de logs de ações que demonstram o cumprimento de direitos do titular, por exemplo, são fundamentais.

3 Hipóteses de Legalidade e Limitação de Finalidade

3.1 Hipóteses de Legalidade para o Tratamento

De acordo com o Artigo 7º da LGPD, o tratamento de dados pessoais só será lícito se, e na medida em que, **pelo menos uma** das hipóteses de legalidade se aplicar:

- mediante o fornecimento de **consentimento** pelo titular;
- para o **cumprimento de obrigação legal ou regulatória** pelo controlador;
- pela **administração pública**, para o tratamento e uso compartilhado de dados necessários à **execução de políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- para a **realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;
- quando necessário para a execução de **contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- para o **exercício regular de direitos** em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- para a **proteção da vida** ou da incolumidade física do titular ou de terceiros;
- para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- quando necessário para atender aos **interesses legítimos** do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente.

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 7º).

Já o tratamento de dados sensíveis não permite a utilização de interesse legítimo nem proteção do crédito como hipóteses de legalidade, mas acrescenta uma hipótese específica, de garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (conforme art. 11 da LGPD).

A lista de hipóteses de legalidade do tratamento é exaustiva, taxativa, e não exemplificativa. Não são possíveis outros motivos legítimos para o tratamento de dados pessoais sob a LGPD.

3.1.1 Limitação de Finalidade e Especificação de Finalidade

As finalidades do tratamento informadas ao titular de dados (em atendimento ao princípio da transparência) devem ser “específicas”, “explícitas” e “legítimas”. Considerando que a LGPD foi inspirada no GDPR, vamos analisar esses três elementos seguindo as orientações do Working Party 29, endossadas pelo European Data Protection Board.

3.1.1.1 Específicas

A fim de determinar se o processamento de dados está em conformidade com a lei e estabelecer quais as salvaguardas de proteção de dados que devem ser aplicadas, a identificação das finalidades específicas é uma pré-condição necessária para a coleta de dados pessoais. A especificação, portanto, estabelece limites para as finalidades para as quais os controladores podem usar os dados pessoais coletados e ajuda a estabelecer as medidas técnicas e administrativas de proteção de dados adequadas e necessárias.

A especificação do propósito requer uma avaliação prévia interna realizada pelo controlador de dados e é uma condição necessária para a prestação de contas. É um primeiro passo fundamental que um controlador deve seguir para garantir a conformidade com a lei de proteção de dados aplicável. O controlador deve identificar quais são as finalidades, documentá-las e demonstrar que realizou essa avaliação interna.

Fonte: Parecer do WP29 sobre limitação de finalidade (acessado em 24 de julho de 2019)

Como a coleta de dados pessoais já é em si um tratando de dados pessoais, a finalidade deve ser especificada antes que a coleta ocorra, sempre que possível.

A especificação de finalidade deve ser detalhada o suficiente para determinar que tipo de tratamento está ou não incluído no objetivo do controlador. Finalidades vagas ou gerais, como "melhorar a experiência dos usuários", "fins de marketing" ou "pesquisas futuras", sem maiores detalhes, geralmente não atendem ao critério de serem "específicas". Uma mensagem para o titular dos dados de que "as informações de navegação são tratadas para apresentar anúncios relacionados aos seus interesses" relacionaria exatamente qual é o objetivo e como é alcançado.

3.1.1.2 Explícitas

Os dados pessoais devem ser coletados para fins explícitos. Os objetivos da coleta não devem ser especificados apenas na mente dos agentes responsáveis pela coleta de dados. Eles também devem ser explicitados. Em outras palavras, as finalidades devem ser claramente reveladas, explicadas ou expressas de alguma forma inteligível. Segue-se da análise anterior que isso deve acontecer, o mais tardar, no momento em que ocorra a coleta de dados pessoais.

O propósito maior deste requisito é garantir que os objetivos do tratamento sejam especificados sem imprecisão ou ambiguidade quanto ao seu significado ou intenção. O que se entende deve ser claro e não deve deixar dúvida ou dificuldade de compreensão. A especificação dos fins deve, em particular, ser expressa de forma a ser entendida da mesma forma não apenas pelo controlador (incluindo todo o pessoal relevante) e por quaisquer terceiros operadores, mas também pelas autoridades de proteção de dados e os titulares de dados em questão. Deve-se tomar cuidado especial para assegurar que qualquer especificação da finalidade seja suficientemente clara para todos os envolvidos, independentemente de suas diferentes origens culturais / linguísticas, nível de compreensão ou necessidades especiais.

Fonte: Parecer do WP29 sobre limitação de finalidade, § III.1.1. (acessado em 30 de março de 2017)

Ao explicitar a finalidade dessa forma, o controlador atende ao princípio da transparência e deixa claro ao titular como pretende utilizar seus dados pessoais. Finalidades explícitas também beneficiam os operadores e informam as autoridades e quaisquer terceiros interessados, de modo que todos tenham um entendimento comum de como os dados podem ser usados. Isso, por sua vez, reduz o risco de que as expectativas dos titulares de dados e/ou de quaisquer interessados sejam diferentes das expectativas do controlador.

3.1.1.3 Legítimas

A exigência de legitimidade significa que as finalidades para o tratamento de dados devem estar de acordo com a lei no sentido mais amplo. Isso inclui todas as formas de direito comum e escrito, legislação primária e secundária, decretos municipais, precedentes judiciais, princípios constitucionais, direitos fundamentais, outros princípios jurídicos, bem como jurisprudência, como tal lei seria interpretada e consideradas pelos tribunais competentes.

Além da legislação de forma geral, o tratamento de dados pessoais deve **sempre** ser baseado em pelo menos uma das hipóteses de legalidade (ver item 3.1).

4 Direitos dos Titulares dos Dados

Desde o histórico de privacidade e proteção de dados, vimos que os direitos fundamentais do titular dos dados são considerados de extrema importância. A LGPD declara que deve haver uma razão legal para o tratamento. O objetivo do tratamento deve ser claramente especificado. E mesmo assim, se houver outros meios além do tratamento de dados pessoais para atingir o objetivo especificado, esses outros meios deverão ser utilizados.

Mesmo quando todos os requisitos são atendidos, o agente de tratamento deve sempre equilibrar os direitos fundamentais do titular de dados com os objetivos do tratamento. Não é de admirar que uma seção relativamente grande da LGPD seja dedicada aos direitos do titular.

4.1 Informação Transparente

Uma ideia básica a LGPD é que o titular de dados deve ser **informado** sempre que seus dados pessoais forem tratados. Se o tratamento for baseado no consentimento, o titular dos dados deve saber e entender com o que está consentindo ('consentimento informado').

Quando o tratamento é baseado em uma ou mais das outras hipóteses de legalidade, o titular de dados ainda deve ser informado sobre quais dados pessoais serão tratados, com que finalidade e quem é responsável. "Saber" e "ser informado" significam, à luz do princípio da transparência da LGPD, "estar ciente" e de fato "entender".
O controlador deve, ainda, informar aos titulares dos dados sobre os direitos que eles têm e ajudá-los a exercer esses direitos. As informações sobre o tratamento pretendido mencionadas anteriormente e a assistência ao titular de dados devem ser fornecidas gratuitamente.

4.2 Informação sobre o Tratamento

O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

- I - finalidade específica do tratamento;
- II - forma e duração do tratamento, observados os segredos comercial e industrial;
- III - identificação do controlador;
- IV - informações de contato do controlador;
- V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- VI - responsabilidades dos agentes que realizarão o tratamento; e
- VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 9º)

4.3 Direto de Acesso e Confirmação sobre o Tratamento

O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- I - confirmação da existência de tratamento;
- II - acesso aos dados;

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 18)

Em primeiro lugar, os controladores podem (e geralmente devem) exigir que os titulares de dados forneçam prova de identidade ao solicitarem a confirmação do tratamento ou, o que é mais crítico, o acesso aos dados pessoais. Isso ajuda a limitar o risco de terceiros obterem acesso ilegal a esses dados.

Pela lei, o titular dos dados tem, a qualquer momento, o direito de obter informações do controlador sobre se os dados pessoais relativos a ele estão sendo tratados ou não.

E se os dados estiverem sendo tratados, o controlador é obrigado a fornecer as informações mencionadas acima e uma cópia dos dados gratuitamente. No entanto, caso haja qualquer abuso no pedido repetitivo e infundado de acesso na forma impressa, é possível que o controlador pleiteie administrativa ou judicialmente a cobrança do custo administrativo do atendimento a esse direito.

Um aspecto importante de se observar é se o direito do titular dos dados de obter uma cópia dos dados pessoais tratados é que a solicitação não pode afetar adversamente os direitos e liberdades de terceiros.

4.4 Outros Direitos

4.4.1 Direito à Correção

Naturalmente, quando um titular de dados tem acesso aos próprios dados pessoais que estão sob responsabilidade do controlador, pode verificar eventualmente que os dados estão incorretos, inexatos ou desatualizados. Nesse caso, o titular dos dados pode exigir uma correção.

4.4.2 Direito à Eliminação

Os titulares de dados têm o direito de ter seus dados "apagados" (eliminados) quando sejam considerados desnecessários, excessivos ou tratados em desconformidade com a LGPD, ou tratados com base no consentimento e já não estejam mais sujeitos a nenhuma hipótese de retenção.

4.4.3 Direito à Anonimização

O titular pode requisitar que os dados desnecessários (inclusive por já não haver mais base legal para o tratamento ou retenção), excessivos ou tratados em desconformidade com a LGPD passem por um processo de anonimização. Isso significa que os atributos que podem identificar direta ou indiretamente o titular serão eliminados de forma segura (sem retorno), e os dados remanescentes não identificarão mais o titular original, deixando de se enquadrar na definição de “dado pessoal” da lei. Tais dados remanescentes podem ser úteis para a composição de estatísticas, por exemplo.

4.4.4 Direito ao Bloqueio do tratamento

O titular poderá requisitar que o tratamento dos dados considerados desnecessários, excessivos ou tratados em desconformidade com a LGPD seja bloqueado, ou seja, suspenso temporariamente.

4.4.5 Direito à Portabilidade dos dados

O titular tem o direito de ter seus dados pessoais brutos transferidos para outro fornecedor de produto ou serviço.

4.4.6 Direito à Revogação do consentimento

Quando o tratamento de dados for baseado no consentimento, o titular poderá, a qualquer momento, e mediante manifestação expressa por procedimento gratuito e facilitado, requisitar a revogação do consentimento, permanecendo válidos os tratamentos realizados anteriormente com base no consentimento que havia sido manifestado, enquanto não houver requerimento de eliminação dos dados.

4.4.7 Direito ao Peticionamento

No que diz respeitoaos seus dados pessoais sob responsabilidade do controlador, o titular pode realizar requerimentos em face do controlador tanto perante a ANPD como perante os órgãos de defesa do consumidor. Estas duas vias são administrativas, e a legislação brasileira ainda assegura a via judicial.

4.4.8 Direito à Oposição ao tratamento

O titular pode requisitar que o tratamento feito com base em uma das hipóteses de dispensa do consentimento e que esteja em desconformidade com a LGPD seja impedido de ser realizado.

4.4.9 Direito à Revisão de decisões automatizadas

As decisões tomadas unicamente com base em tratamento automatizado de dados pessoais e que afetem os interesses do titular dos dados poderão ser revisadas – incluindo-se as decisões que tem por finalidade definir o perfil pessoal, profissional, de consumo e de crédito do titular, ou aspectos da sua personalidade.

5 Incidentes com Dados Pessoais e Procedimentos Relacionados

5.1 O Conceito de Incidentes com Dados Pessoais

Incidentes com dados pessoais são incidentes de segurança que envolvem dados pessoais. Em outras palavras, são eventos que afetem pelo menos um dos três principais pilares de segurança da informação em relação a dados pessoais:

"(i) confidencialidade, ou seja, a garantia de que as informações (no caso, os dados pessoais) somente serão acessados pelas pessoas devidamente autorizadas para tanto; (ii) integridade, o que significa a garantia de que os dados não serão modificados sem autorização, e (iii) disponibilidade, ou a garantia de que os dados poderão ser acessados pelas pessoas autorizadas sempre que houver necessidade."

Fonte: https://cryptoid.com.br/protecao-de-dados/serie-dicas-praticas-para-implementacao-de-privacy-by-design-parte-iii-de-iv/. Acesso em 09.01.2021.

O incidente com dados pessoais é a uma situação em que os dados pessoais são tratados de forma não autorizada e, portanto, ilegalmente. Nem todo incidente de segurança envolve dados pessoais. Lembre-se de que acessar, copiar, armazenar e destruir também são considerados tratamentos (qualquer tipo de operação com dados pessoais).

Dessa forma, por exemplo, um incêndio em um data center pode destruir os dados pessoais armazenados lá. Isso tornaria um incidente de segurança com dados pessoais, porque feriu o pilar da disponibilidade de segurança da informação (os dados agora não são mais acessíveis) e constitui um tratamento não autorizado (a destruição dos dados).

De maneira semelhante, quando um operador exclui acidentalmente (e sem retorno) um conjunto de dados pessoais, também fere o pilar da disponibilidade e causa um incidente com dados pessoais.

Vale ressaltar que "incidentes", de forma geral, podem se referir à quebra de confidencialidade, integridade e/ou disponibilidade de dados em geral, inclusive de estratégias e segredos comerciais. Por isso, é importante verificar no contexto do incidente se havia de fato dados pessoais envolvidos para aplicação da LGPD.

É fundamental aplicar medidas técnicas e administrativas para mitigar riscos e evitar, ao máximo, que ameaças de fato consigam explorar vulnerabilidades, materializando incidentes. Sobre os conceitos de “ameaça”, “vulnerabilidade” e “risco”, podemos defini-los da seguinte forma:

“A ameaça é um evento ou atitude, interna ou externa à organização, que, em geral, foge do controle da organização e tem o potencial de ferir pelo menos um dos pilares de segurança da informação. Por exemplo, um incêndio que torna indisponíveis os dados registrados nos papéis queimados (e que não estivessem registrados em nenhum outro lugar) ou a atuação de um hacker que copia dados e os compartilha com terceiros sem autorização.

Já a vulnerabilidade é uma “fraqueza” ou “falha” que tem o potencial de comprometer pelo menos um dos pilares de segurança da informação, devendo ser mapeada e minimizada ou eliminada o quanto antes possível.

O risco, por sua vez, é o resultado da probabilidade de um evento acontecer (no caso, de uma ameaça explorar uma vulnerabilidade) conjugado com o nível de impacto ou dano que pode causar se de fato vier a ocorrer.”

Fonte: https://cryptoid.com.br/protecao-de-dados/serie-dicas-praticas-para-implementacao-de-privacy-by-design-parte-iii-de-iv/. Acesso em 09.01.2021.

5.2 Procedimento sobre como agir quando ocorre incidente com dados pessoais

De acordo com o artigo 46 da LGPD, os agentes de tratamento (controlador e operadores, quando houver) devem adotar medidas de segurança, técnicas e administrativas, adequadas para proteger os dados pessoais contra acessos ou quaisquer outros tratamentos não autorizados, acidentais ou intencionais, como a destruição, perda, alteração, comunicação ou qualquer forma de tratamento ilícito.

Melhores práticas internacionais de segurança da informação, como os frameworks NIST e ISO (com destaque para a ISO 27001 e suas derivadas), são amplamente aceitos e recomendados para as organizações cumprirem com os princípios da segurança e prevenção e atenderem ao artigo 49 da LGPD (os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos padrões de boas práticas). Esses frameworks, inclusive, contêm diretrizes para orientar procedimentos de resposta a incidentes.

5.2.1 Notificação de um incidente com dados pessoais à ANPD e ao titular de dados

De acordo com o artigo 48 da LGPD, quem comunica o incidente à Autoridade Nacional de Proteção de Dados é o controlador. Isso significa que, caso o incidente com dados pessoais ocorra no âmbito da operação do operador, este (o operador) tem obrigação de comunicar o controlador, para que o controlador, então, tome as devidas providências e comunique à ANPD e aos titulares, quando cabível.

Vale destacar que, segundo a redação do artigo 48, não é necessário comunicar à ANPD e aos titulares de dados todo e qualquer tipo de incidente com dados pessoais, mas somente aqueles que **possam acarretar risco ou dano relevante aos titulares**, que possam resultar em danos materiais ou imateriais aos titulares, tais como perdas financeiras, danos à reputação, limitação de direitos, discriminação, roubo de identidade ou fraude.

Os outros tipos de incidente com dados pessoais que não se enquadrem nessa definição (porque, por exemplo, os dados estavam criptografados/ilegíveis e/ou foram tomadas medidas eficazes para minimizar qualquer risco para os titulares) não precisam ser comunicados nem à ANPD nem aos titulares de dados. No entanto, e em atendimento ao princípio da responsabilização e

prestação de contas, é necessário que mesmo esses incidentes menos relevantes com dados pessoais sejam comunicados pelo operador ao controlador, para que o controlador atenda ao princípio da responsabilização e possa tomar as medidas cabíveis, ainda que para melhoria do fluxo de tratamento e reforço da segurança.

Sobre a comunicação à ANPD e aos titulares de dados, a LGPD estabelece que deverá ser feita em "prazo razoável", não havendo, ainda, nenhuma especificação pela ANPD quanto ao que significa essa expressão. Na falta de uma diretriz sobre o prazo, muitas organizações têm feito uma analogia ao prazo do GDPR e ajustado seus procedimentos internos para que a comunicação seja feita dentro de 72 (setenta e duas) horas após a tomada de conhecimento em relação ao incidente.

O texto da comunicação deverá conter, no mínimo, as seguintes informações:

- I - a descrição da natureza dos dados pessoais afetados;
- II - as informações sobre os titulares envolvidos;
- III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente;
- V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 48, §1º)

Ao analisar a comunicação, a ANPD deverá verificar a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

A LGPD estabelece, ainda, que, na análise da gravidade do incidente, a ANPD deverá avaliar eventuais provas de que os agentes de tratamento adotaram medidas técnicas adequadas para tornar os dados pessoais afetados no âmbito e nos limites técnicos de seus serviços, ininteligíveis, para terceiros não autorizados a acessá-los, pois essas medidas devem reduzir o nível de impacto aos titulares e, consequentemente, também devem reduzir o nível de gravidade do incidente.

Organizando a Proteção de Dados

6 Importância da proteção de dados para a organização

Quase todas as organizações tratam dados pessoais. Para uma organização que trata dados pessoais, a proteção de dados não é apenas "um requisito da lei" ou "importante para evitar multas", mas algo diretamente vinculado à sua reputação e à confiança do cliente/consumidor.

O tratamento de dados pessoais realizado de maneira adequada significa garantia de qualidade, gerenciamento de segurança e governança.

Os parágrafos a seguir destacam alguns dos requisitos que não podem faltar para o que tratamento de dados pessoais seja considerado adequado.

6.1 Requisitos para o tratamento adequado

6.1.1 Cumprimento dos princípios relativos ao tratamento de dados pessoais

Os princípios de proteção de dados estabelecidos no artigo 6º da LGPD não apenas devem cumpridos como deve haver formas efetivas (documentadas) de comprovar esse cumprimento. O objetivo deve ser claro, detalhado e especificado, e pelo menos uma das possíveis “hipóteses legais para o tratamento” deve ser aplicada. Os direitos do titular de dados devem ser garantidos e medidas adequadas de proteção de dados devem ser aplicadas.

6.1.2 Estrutura legal

O controlador, como agente que determina as finalidades e a forma de tratamento, é obrigado a implementar medidas técnicas e organizacionais apropriadas para assegurar que o tratamento seja realizado de acordo com a LGPD, não apenas no âmbito de sua operação, mas também de quaisquer operadores que eventualmente contrate. E, para garantir que o nível de proteção de dados se mantenha o mesmo em toda a cadeia de tratamento, é fundamental que o controlador também garanta, por meio do contrato com o operador, previsões de que o operador somente poderá terceirizar parte do tratamento (para um sub-operador) em casos já previstos e autorizados no contrato ou, caso contrário, a terceirização deverá ser autorizada pelo controlador antes de ocorrer.

O operador somente deverá tratar os dados pessoais baseado nas instruções documentadas do controlador. É obrigatória a existência de um contrato juridicamente vinculante entre o operador e o controlador e que defina:

- o objeto do tratamento
- a duração do tratamento
- a natureza e o objetivo do tratamento, como definido pelo controlador
- os tipos de dados pessoais envolvidos
- as categorias de titulares de dados afetados
- as obrigações, responsabilidades e direitos dos agentes de tratamento

Durante a relação entre controlador e operador, é importante que ambos consigam **demonstrar conformidade** com os requisitos da LGPD, e isso pode ser feito por meio da **documentação de provas de conformidade**.

6.1.3 Relatório de Impacto à Proteção de Dados (RIPD)

Pela lei, realizar um RIPD não é obrigatório para todos os tipos de tratamento, mas somente para aqueles que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Ainda assim, para os casos que não geram esses riscos, é uma boa prática documentar a análise e fundamentação do motivo pelo qual o tratamento não se encaixa nessa obrigatoriedade, e muitas vezes isso pode ser realizado no próprio formato de um RIPD. O que um RIPD compreende e seus objetivos são discutidos no tópico 8.3.

6.1.4 Contrato entre controlador e operador

Quando o controlador quiser terceirizar parte da operação de tratamento para outra parte, um operador, um contrato jurídico válido deve ser previamente assinado entre as partes. Os detalhes do contrato são descritos no tópico 8.2.

6.2 Tipos Requeridos de Administração

De acordo com o princípio da responsabilização e prestação de contas, o agente de tratamento deve manter registros capazes de demonstrar e comprovar a adoção de medidas eficazes para a proteção de dados pessoais. Nesse sentido, há dois tipos de registros que são fundamentais.

6.2.1 Registro de atividades de tratamento

O registro deve conter:

(a) O nome e detalhes de contato do(s) agentes de tratamento envolvidos, seus representantes e DPOs (Encarregados);
(b) as finalidades do tratamento;
(c) a descrição das categorias de titulares de dados e categorias de dados pessoais;
(d) as categorias de destinatários a quem tenham sido ou venham a ser divulgados os dados pessoais, incluindo destinatários em países terceiros ou organizações internacionais;
(e) quando aplicável, as transferências de dados pessoais para um país terceiro ou uma organização internacional, incluindo a identificação desse país ou organização internacional;
(f) sempre que possível, os prazos previstos para a eliminação segura das diferentes categorias de dados, e
(g) sempre que possível, uma descrição geral das medidas técnicas e organizacionais de segurança da informação existentes.

6.2.2 Registro de incidentes com dados pessoais

Conforme recomendado pelas melhores práticas de segurança da informação, os agentes de tratamento devem registrar quaisquer incidentes que eventualmente ocorram com dados pessoais sob sua responsabilidade, mesmo que não haja necessidade de comunicação do evento à ANPD e aos titulares dos dados.

Algumas das informações que devem ser registradas são:

- Nome e detalhes de contato do DPO (Encarregado) ou de outro junto a quem maiores informações podem ser obtidas;
- A natureza do incidente com dados pessoais;
- As categorias e o número aproximado de titulares de dados afetados;
- As categorias e número aproximado de registros de dados pessoais afetados;
- As prováveis consequências em termos de risco para os direitos e liberdades das pessoas naturais, e
- As medidas tomadas ou a tomar para resolver as consequências do incidente com dados pessoais.

7 Autoridade Nacional de Proteção de Dados (ANPD)

De acordo com o artigo 5º, inciso XIX, e com os artigos 55-A e 55-B, a ANPD é o órgão da administração pública federal, integrante da Presidência da República, com autonomia técnica e decisória, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

É composta por um Conselho Diretor, órgão máximo de direção, um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, a Corregedoria, a Ouvidoria, um órgão de assessoramento jurídico próprio e unidades administrativas ou especializadas necessárias à aplicação da LGPD (conforme o art. 55-C, LGPD).

7.1 Responsabilidades Gerais de a ANPD

A principal responsabilidade de a ANPD é zelar pela proteção dos dados pessoais, nos termos da legislação (art. 55-J, inciso I, LGPD), ou seja, **fiscalizar e fazer cumprir a aplicação** da LGPD com o objetivo de **proteger** os direitos e liberdades fundamentais das pessoas naturais em relação ao tratamento.

Outra importante responsabilidade é promover a conscientização pública e a compreensão dos riscos, regras, salvaguardas e direitos em relação ao tratamento de dados pessoais.

A lista de competências detalhadas no Artigo 55-J da LGPD é longa e aberta. Abaixo as várias competências foram resumidas em alguns pontos de destaque.

7.1.1 Acompanhar e fazer cumprir a aplicação da lei

A ANPD fiscaliza a aplicação da LGPD.

Isso pode ter um aspecto **preventivo**, fiscalizando desenvolvimentos relevantes ou conduzindo investigações, sempre que possam gerar impacto na proteção de dados pessoais.

Pode também ter um aspecto **remediador**, investigando operações de tratamento que infringiram a lei, incluindo investigações baseadas em reclamações de titulares de dados, organizações ou associações e em informações recebidas de outra autoridade pública.

7.1.2 Aconselhar e promover a conscientização

Uma das competências de atuação da ANPD é promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança, e promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade. Também pode emitir orientações e elaborar diretrizes na matéria.

7.1.3 Administrar incidentes com dados pessoais e outras infrações

Cabe à ANPD receber as comunicações dos controladores sobre incidentes com dados pessoais, bem como fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

7.1.4 Estabelecer Padrões

A ANPD tem a responsabilidade de estabelecer normas e diretrizes para os temas sem definições no texto da LGPD.

7.1.4.1 Cláusulas-padrão contratuais, normas corporativas globais, selos, certificados e códigos de conduta

De acordo com o artigo 35 da LGPD, compete à ANPD a definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta.

7.2 Papeis e Responsabilidades Relacionadas a Incidentes de Segurança com Dados Pessoais

Quando a ANPD recebe uma notificação de um incidente de segurança com dados pessoais, deve avaliar a gravidade do ocorrido e como a proteção de dados foi implementada pelo controlador e pelo operador ou operadores envolvidos.

A avaliação dos riscos para os titulares dos dados e as medidas mitigadoras que já foram ou ainda devem ser tomadas são claramente urgentes.

Em princípio, o controlador é responsável por:

- investigar o incidente com dados pessoais, as circunstâncias em que ocorreu
- realizar a avaliação dos riscos envolvidos para os titulares de dados
- adotar medidas de mitigação para minimizar as consequências negativas para os direitos e liberdades dos titulares dos dados e de outras pessoas envolvidas.

No entanto, a ANPD pode receber amplos poderes para monitorar essa investigação e ordenar que os controladores e operadores envolvidos tomem outras medidas ou medidas extras para alinhar as operações de tratamento com a LGPD e até para restringir ou bloquear o tratamento.

7.3 Poderes da Autoridade Nacional de Proteção de Dados (ANPD) na aplicação da LGPD

Uma das principais responsabilidades da ANPD é fazer **cumprir** a aplicação da LGPD. Além dos poderes consultivos, a ANPD possui amplos poderes de investigação e correção para impor a implementação da LGPD. Isso inclui, quando necessário, a aplicação de multas e outras sanções administrativas.

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

Fonte: art. 5º, inciso XIX, LGPD.

7.3.1 Poderes de investigação da ANPD

O Artigo 55-J, inciso IV, da LGPD concede à ANPD poder de fiscalizar e aplicar sanções. Dentre as previsões do artigo citado, bem como de outros dispositivos da LGPD, ela tem o poder:

- fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- realizar auditorias, ou determinar sua realização, no âmbito das atividades de fiscalização;
- solicitar ao controlador relatório de impacto à proteção de dados pessoais, inclusive quando o tratamento tiver como fundamento seu interesse legítimo;
- realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

7.3.2 Poderes corretivos da ANPD

O Artigo 52, da LGPD concede à ANPD poderes de correção para:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, 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;
- multa diária, observado o limite total do valor acima;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- 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 infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

7.3.3 Condições gerais para a imposição de multas administrativas

As multas administrativas devem ser proporcionais e dissuasivas, levando em consideração as peculiaridades do caso concreto.

7.3.3.1 Proporcional

Quando a ANPD decidir impor uma multa administrativa, além de outras medidas, ela deve dar a devida atenção às circunstâncias.

Os critérios para essa decisão são:

- a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- a boa-fé do infrator;
- a vantagem auferida ou pretendida pelo infrator;
- a condição econômica do infrator;
- a reincidência;
- o grau do dano;
- a cooperação do infrator;
- a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;
- a adoção de política de boas práticas e governança;
- a pronta adoção de medidas corretivas; e
- a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

A cooperação com a ANPD para remediar uma infração e mitigar os possíveis efeitos adversos da infração poderá ser favorável aos controladores e operadores.

7.3.3.2 Dissuasivo

Uma multa também deve ser dissuasiva. Qualquer que seja o custo da implementação de medidas para cumprir a LGPD em uma organização, nenhuma empresa deve arriscar ignorar as regras, porque as multas vão muito além do que custará a conformidade. Ainda assim, a intenção é incentivar as empresas a cumprir a LGPD, e não as destruir financeiramente.

7.4 Transferência Internacional de Dados

7.4.1 Definição

A transferência de dados é, segundo o inciso X do artigo 5º da LGPD, um tipo de tratamento, pois constitui uma operação realizada com dados pessoais. Já a transferência internacional de dados é definida pelo inciso XV do mesmo artigo como:

> Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro
>
> Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 5º, XV)

7.5 Normas aplicáveis à transferência internacional de dados

Em geral, as transferências de dados entre fronteiras para um destinatário em um país terceiro só podem ocorrer se a transferência for feita para uma 'jurisdição adequada' ou se a parte ou partes que exportam os dados tiverem implementado um mecanismo legal de transferência de dados.

7.5.1 Transferências para país ou organismo avaliado pela ANPD como adequado

> A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; [...] Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.
>
> Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 33)

A ANPD precisa analisar e garantir que o país ou organismo destinatário dos dados pessoais objeto de transferência apresenta um nível adequado de proteção de dados pessoais em razão de sua legislação interna ou dos compromissos internacionais assumidos.

7.5.2 Transferências sujeitas a salvaguardas apropriadas

Na ausência de uma aprovação do país ou organismo internacional pela ANPD, o controlador ou o operador deve tomar medidas para compensar a falta de proteção de dados em um país terceiro por meio de aplicação de salvaguardas (garantias) apropriadas para o titular dos dados.

Essas salvaguardas adequadas podem consistir na utilização de cláusulas contratuais específicas para determinada transferência, normas corporativas globais, cláusulas-padrão contratuais, bem como selos, certificados e códigos de conduta regularmente emitidos. A definição do conteúdo de cláusulas-padrão contratuais e a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta serão realizadas pela ANPD.

Essas salvaguardas devem garantir a conformidade com os requisitos de proteção de dados e os direitos dos titulares de dados adequados ao tratamento em conformidade com a LGPD.

Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (arts. 34 e 35)

7.5.3 Normas Corporativas Globais (NCG)

As NCG têm origem nas regras corporativas vinculantes, instituídas pelo GDPR:

Um grupo de empresas, ou um grupo de empresas envolvidas numa atividade econômica conjunta, deve poder utilizar as regras empresariais vinculantes aprovadas para as suas transferências internacionais da União para organizações pertencentes ao mesmo grupo de empresas ou grupo de empresas uma atividade econômica conjunta, desde que tais regras corporativas incluam todos os princípios essenciais e direitos aplicáveis para garantir as salvaguardas apropriadas para transferências ou categorias de transferências de dados pessoais.

Fonte: item 110 do Preâmbulo do GDPR.

As Normas Corporativas Globais devem:

- ser juridicamente vinculantes;
- ser aplicadas e reforçadas por todos os membros envolvidos do grupo, incluindo seus empregados;
- conferir expressamente direitos aplicáveis aos titulares dos dados no que diz respeito ao tratamento dos seus dados pessoais;
- estender os requisitos de proteção de dados estabelecidos na LGPD para todo o grupo.

Dentre os requisitos da LGPD, as Normas Corporativas Globais (NCG) devem especificar pelo menos:

- as transferências de dados, categorias de dados, tipos de tratamento e suas finalidades;
- tipos de titulares de dados afetados e identificação do país ou organismo internacional destinatário;
- a aplicação dos princípios gerais de proteção de dados e os requisitos relativos a transferências subsequentes para organismos não vinculados pelas normas corporativas globais das empresas;
- os direitos das pessoas afetadas em relação ao tratamento e os meios para exercer esses direitos;
- a aceitação da responsabilidade por eventuais infrações às normas corporativas globais da empresa;
- o mecanismo de cooperação com a ANPD para assegurar o cumprimento por qualquer membro do grupo.

Prática de Proteção de Dados

8 Aspectos de qualidade

8.1 Proteção de Dados desde a Concepção (by design) e por Padrão (by default)

> Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito. [Essas medidas] deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
>
> Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 46, caput e § 2º)

Com este artigo, a LGPD faz do princípio de proteção de dados **desde a concepção** (by design) um **requisito legal**, e não apenas uma maneira eficaz de cumprir as obrigações relacionadas à segurança dos dados. O controlador é responsável pela implementação de um conjunto completo de medidas técnicas e administrativas **apropriadas**.

O controlador deve implementar medidas técnicas e administrativas apropriadas para garantir que, **por padrão** (by default), apenas sejam tratados os dados pessoais estritamente necessários para cada finalidade específica do tratamento. Isso se aplica à quantidade de dados pessoais coletados, à extensão de seu tratamento, ao período de armazenamento e à acessibilidade.

Além disso, o conjunto de medidas técnicas e administrativas apropriadas é necessário para integrar as salvaguardas necessárias ao tratamento para proteger os direitos dos titulares de dados. Dessa forma, uma ligação jurídica é definida entre os princípios de segurança de dados e a privacidade, com o objetivo de garantir a efetividade do direito humano à privacidade.

8.1.1 Os sete princípios de privacidade desde a concepção (by design)

A ideia de privacidade desde a concepção (by design) foi desenvolvida por Ann Cavoukian, PhD., ex-Comissária de Informações e Privacidade, em Ontário, Canadá. Em uma publicação sobre os princípios, ela escreveu:

> Privacidade desde a concepção (by design) é um conceito que desenvolvi nos anos 90, para abordar os efeitos sempre crescentes e sistêmicos das Tecnologias de Informação e Comunicação e dos sistemas de dados em rede em larga escala. A Privacidade desde a concepção (by design) promove a visão de que o futuro da privacidade não pode ser assegurado apenas pelo cumprimento de estruturas regulatórias; em vez disso, a garantia da privacidade deve idealmente se tornar o modo de operação padrão de uma organização.
>
> Fonte: Ann Cavoukian. 2011. Privacy by Design, the 7 foundational principles

O framework de privacidade desde a concepção (by design) é composto por sete princípios, que serão explorados próximos parágrafos.

8.1.1.1 Proativo não reativo; preventivo não corretivo

A abordagem de privacidade desde a concepção (by design) é caracterizada por medidas proativas em vez de reativas. Ele antecipa e evita eventos invasivos à privacidade antes que eles aconteçam. A privacidade desde a concepção (by design) não espera que os riscos à privacidade se concretizem, nem oferece remédios para resolver infrações à privacidade depois de terem ocorrido - ele visa **impedir** que ocorram. Em resumo, a privacidade desde a concepção (by design) vem antes do fato, não depois.

8.1.1.2 Privacidade como configuração padrão (by default)

Todos podem ter certeza de uma coisa: as regras padrão. A Privacidade desde a concepção (by design) busca oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática comercial. Se um indivíduo não faz nada, sua privacidade permanece intacta. Nenhuma ação é necessária por parte de um titular de dados para proteger sua privacidade. Privacidade e proteção de dados são incorporadas ao sistema, por padrão.

8.1.1.3 Privacidade Incorporada ao Design

A Privacidade desde a concepção (by design) está incorporada ao design e à arquitetura de sistemas de TI e práticas de negócios. Não é acoplada como um complemento após o fato. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que será entregue. A privacidade é parte integrante do sistema, sem diminuir suas funcionalidades.

8.1.1.4 Funcionalidade Total - Soma Positiva, Não Soma Zero

A Privacidade desde a concepção (by design) busca acomodar todos os interesses e objetivos legítimos de uma maneira positiva para todos, não por meio de uma abordagem de soma zero, em que compensações desnecessárias são feitas. A Privacidade desde a concepção (by design) evita a pretensão de falsas dicotomias, como privacidade versus segurança, demonstrando que é possível ter ambas.

8.1.1.5 Segurança de ponta a ponta - proteção total do ciclo de vida dos dados

A Privacidade desde a concepção (by design) tendo sido incorporada ao sistema antes do primeiro elemento da informação que está sendo coletada, se estende com segurança durante todo o ciclo de vida dos dados envolvidos - medidas de segurança fortes são essenciais à privacidade, do início ao fim. Isso garante que todos os dados sejam retidos com segurança e, em seguida, destruídos com segurança (sem possibilidade de recuperação) no final do processo, em tempo hábil. Assim, a Privacidade desde a concepção (by design) garante o gerenciamento do ciclo de vida de dados pessoais seguro e de ponta a ponta.

8.1.1.6 Visibilidade e transparência

A Privacidade desde a concepção (by design) procura assegurar a todas as partes interessadas que, seja qual for a prática ou tecnologia de negócio envolvida, ela está, de fato, operando de acordo com as promessas e objetivos declarados, sujeita à verificação independente. Seus componentes e operações permanecem visíveis e transparentes para usuários e provedores.

8.1.1.7 Respeito pela privacidade do usuário

Acima de tudo, a Privacidade desde a concepção (by design), exige que os arquitetos e operadores mantenham os interesses do indivíduo (usuário) em primeiro lugar, oferecendo medidas como padrões de privacidade fortes, notificação apropriada e capacitando opções fáceis de usar. O objetivo é garantir que se mantenha o foco no usuário.

8.1.2 Benefícios da aplicação dos princípios de Privacidade desde a concepção (by design) e por padrão (by default)

Em seu site, o Gabinete do Comissário de Informação do Reino Unido[3] escreveu:

Adotar uma abordagem de Proteção de Dados desde a Concepção (by design) é uma ferramenta essencial para minimizar os riscos à privacidade e criar confiança. Criar projetos, processos, produtos ou sistemas com a privacidade em mente desde o início pode levar a benefícios que incluem:

- problemas potenciais são identificados em um estágio inicial, quando resolvê-los será sempre mais simples e menos dispendioso;
- maior conscientização sobre privacidade e proteção de dados em toda a organização;
- as organizações são mais propensas a cumprir suas obrigações legais e menos propensas a violar a legislação de proteção de dados;
- é menos provável que as ações sejam invasivas à privacidade e tenham um impacto negativo nos indivíduos.

8.2 Contratos entre Controlador e Operador

Conforme visto no item 8.1 acima, o Artigo 46 da LGPD exige que tanto o controlador como o operador implementem medidas técnicas e administrativas apropriadas e garantam que essas precauções permaneçam em vigor durante o tratamento, na verdade, implementando um dos princípios da Proteção de Dados desde a Concepção (by design): o de segurança de ponta-a-ponta.

Dessa forma, quando um operador é contratado para executar o tratamento ou parte do tratamento em nome do controlador, o contrato por escrito entre esses agentes deve garantir que o mesmo nível de segurança e compliance em proteção de dados seja aplicado em toda a cadeia de tratamento.

8.2.1 Cláusulas do contrato

A LGPD não determina o conteúdo específico que deveria constar no contrato entre Controlador e Operador. No entanto, O Artigo 28(3) do GDPR (Regulamento em que nossa lei se inspirou), determina que esse contrato (ou outro ato jurídico que vincule os agentes de tratamento) deve estipulas, em especial, que o operador (“tratador”, no GDPR):

(a) processe os dados pessoais apenas conforme as instruções documentadas do controlador, incluindo no que diz respeito às transferências de dados pessoais para um país terceiro ou uma organização internacional;
(b) assegure que as pessoas autorizadas a tratar os dados pessoais se comprometeram com a confidencialidade ou estejam sujeitas a uma obrigação legal adequada de confidencialidade;
(c) adote todas as medidas técnicas e administrativas de segurança do tratamento, conforme determinado pelo artigo 46 da LGPD;
(d) respeite as condições impostas pelo Controlador para contratar outro operador (também chamado de “sub-operador”);
(e) auxilie o controlador, por meio de medidas técnicas e administrativas apropriadas, na medida do possível, no cumprimento da obrigação do controlador de responder aos pedidos de exercício dos direitos de titulares de dados;
(f) auxilie o controlador a garantir o cumprimento das obrigações de segurança, notificações às autoridades, notificações aos titulares de dados e elaboração de Relatório de impacto à

[3] Fonte: https://ico.org.uk/. Acesso em: 25.04.2017.

Proteção de Dados, considerando a natureza do tratamento e as informações de que dispõe;

(g) à escolha do controlador, suprima ou devolva todos os dados pessoais ao controlador após o termo da prestação de serviços relacionados ao tratamento e elimine eventuais cópias existentes, a menos que a legislação exija a conservação dos dados pessoais, e

(h) disponibilize ao controlador todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas, permitindo e contribuindo para as auditorias, incluindo as inspeções realizadas pelo controlador ou por outro auditor à mando do controlador.

(i) Ressalta-se que esse conteúdo, ainda que seja determinado pela legislação europeia (GDPR), tem sido amplamente adotado pelo mercado brasileiro na ausência de orientação pela LGPD ou pela ANPD.

8.2.1.1 Exemplo

A tabela a seguir mostra um exemplo do conteúdo que um contrato de tratamento de dados entre o controlador e o operador deveria abordar:

Conteúdo	Referência GDPR (podem ser aplicadas analogamente ao cenário brasileiro)
Escopo e finalidade do contrato	Artigo 4(2) definições: processamento(tratamento)
Dados cobertos pelo acordo	Artigo 4(1) dados pessoais; Artigo 9 / item 10 categorias especiais de dados pessoais (dados sensíveis);
Segurança geral e salvaguardas no tratamento de dados	Artigo 32 segurança do processamento (tratamento)
Medidas técnicas e administrativas	Artigo 28(3, “a” até “h”)
Monitoramento da segurança da informação e proteção de dados	Artigo 35 avaliação (relatório) de impacto sobre proteção de dados
Violação de segurança da informação e incidente com dados pessoais	Artigo 33(2) notificação de um incidente com dados pessoais à autoridade e aos titulares
Correção, exclusão e bloqueio / obrigações específicas para auxiliar o controlador	Artigo 32.36
Acordo com outro operador de dados	Artigo 28(2) e (4) subprocessador (sub-operador)
Transferência de dados	Rec. (112), (113); Artigo 47 Regras Corporativas Vinculantes (Normas Corporativas Globais); Artigo 49 exceções para situações específicas; o capítulo V transfere (..) para países terceiros ou organizações internacionais.
Outras obrigações do operador	Artigo 39 tarefas do DPO; (1b)... sensibilização e formação do pessoal envolvido nas operações de processamento(tratamento)
Os direitos de controle dos controladores	Artigo 4(7) controlador Artigo 28(3f) suporte ao controlador ...
Retorno e exclusão dos dados pessoais	Artigo 28(3g) eliminar ou devolver
Dever de confidencialidade	Artigo 28(3b) confidencialidade
Duração	Artigo 28(3) duração do processamento(tratamento) Artigo 5 princípios relativos ao processamento (tratamento) de dados pessoais (1) (e) limitação de armazenamento
Prevalência	No caso de cláusulas conflitantes, legislação tem prevalência
Assinaturas	

8.3 Relatório de Impacto sobre a Proteção de Dados (RIPD)

O primeiro princípio de Proteção de Dados desde a Concepção (by design) requer que o controlador antecipe e evite eventos danosos às liberdades civis e direitos fundamentais (com destaque para a privacidade) e antes que eles ocorram.

A LGPD inclui essa determinação no Artigo 5º, XVII:

> 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.
>
> Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 5º, inciso XVII)

A LGPD não exige que um RIPD seja executado para cada operação de tratamento. Na realidade, o texto da lei é bem sucinto na matéria. Em resumo, afirma: (i) que a ANPD poderá solicitar ao controlador que apresente RIPD quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (artigo 10, § 3º, LGPD), e (ii) que a ANPD poderá determinar ao controlador que elabore RIPD para o tratamento de dados pessoais, inclusive de dados sensíveis, observados os segredos comercial e industrial (artigo 38, *caput*, LGPD).

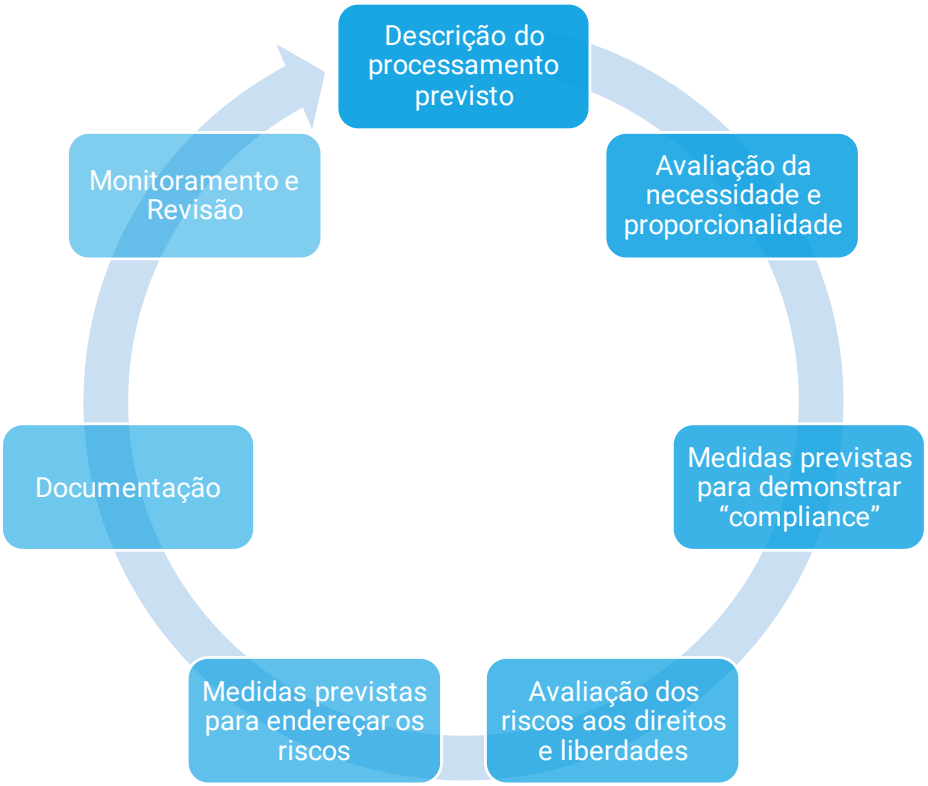
Ainda no artigo 38, parágrafo único, acrescenta que relatório deverá conter, no mínimo:

(a) a descrição dos tipos de dados coletados;
(b) a metodologia utilizada para a coleta e para a garantia da segurança das informações, e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Ainda não há diretrizes oficiais brasileiras sobre a realização de um RIPD, mas é possível aplicar, por analogia, algumas orientações europeias sobre o DPIA. Por exemplo, não há impeditivo legal na LGPD para que um RIPD pode enderece um conjunto de operações de tratamento semelhantes de uma só vez. Isso significa que **um único RIPD poderia ser usado para avaliar várias operações de tratamento que são semelhantes em termos dos riscos apresentados**, desde que seja dada consideração adequada à natureza específica, ao escopo, ao contexto e às finalidades do tratamento. Isso pode significar, por exemplo, um único relatório para onde uma tecnologia semelhante é usada com a finalidade de coletar o mesmo tipo de dados para os mesmos fins.

Aplicando-se a abordagem de *privacy by design*, o RIPD deve ser realizado **antes de o ser realizado tratamento**. Isso porque a análise evidenciará eventuais riscos às liberdades civis e aos direitos fundamentais em uma fase em que menos danoso (ao titular de dados) mitigar esses riscos, assim como é também e menos custoso e mais fácil para o agente corrigir o projeto de um novo produto ou serviço em fase embrionária.

O RIPD, portanto, deve ser iniciado **o mais cedo possível** no projeto da operação de tratamento, mesmo que algumas das operações de tratamento ainda sejam desconhecidas. À medida que o RIPD for atualizado durante todo o projeto de ciclo de vida, ele garantirá que a proteção de dados e a privacidade sejam consideradas e que sejam criadas soluções que promovam a conformidade. Também é necessário repetir etapas individuais dessa avaliação à medida que o processo de desenvolvimento avança, porque a seleção de certas medidas técnicas ou administrativas pode afetar a gravidade ou a probabilidade dos riscos representados pelo tratamento.



O fato de que o RIPD pode precisar ser atualizado uma vez que o tratamento tenha realmente iniciado **não** é uma razão válida para adiar ou não executar um RIPD. Em alguns casos, o RIPD será um processo contínuo, por exemplo, quando uma operação de tratamento é dinâmica e está sujeita a alterações contínuas. Executar um RIPD é um processo contínuo, não um exercício único[4].

8.3.1 Objetivos de um RIPD

Existem vários motivos para realizar um RIPD - como a ideia de prevenção, conforme vista em um dos princípios de Privacidade desde a Concepção (by design), bem como a obrigação de documentar a conformidade, e outros. Em detalhes, um RIPD ajudará a:

- evitar mudanças dispendiosas nos processos, redesenho de sistemas ou encerramento de projetos;
- reduzir as consequências da supervisão e fiscalização;
- melhorar a qualidade dos dados;
- melhorar a prestação de serviços;
- melhorar a tomada de decisão;
- aumentar a conscientização sobre privacidade em uma organização;
- melhorar a viabilidade do projeto;
- melhorar a comunicação em relação à privacidade e proteção de dados pessoais, e
- reforçar a confiança dos titulares de dados na forma como os dados pessoais são tratados e a privacidade é respeitada.

[4] Figura adaptada de Guidelines on Data Protection Impact Assessment (DPIA), WP29 document 17/EN/248.

8.3.2 Tópicos de um RIPD

A LGPD não estabelece as características mínimas de um RIPD. Recorre-se, novamente, ao GDPR (Artigo 35(7) e itens 84 e 90) para orientação, no silêncio da legislação nacional:

- uma descrição das operações de tratamento previstas e as finalidades do tratamento;
- uma avaliação da necessidade e proporcionalidade do tratamento;
- uma avaliação dos riscos para os direitos e liberdades dos titulares de dados, e
- as medidas previstas para:
    - abordar os riscos, e
    - demonstrar o cumprimento com a legislação.

8.4 Gestão do Ciclo de Vida de Dados (GCVD)

Independentemente de os dados serem gerados por e dentro da organização ou coletados pela organização por meio de terceiros (cliente, fornecedor, parceiro), a única maneira de protegê-los é entendê-los. Eles contêm informações pessoais de qualquer tipo, como sobre clientes, funcionários, comunicações confidenciais, informações de identificação pessoal, informações sobre saúde ou dados financeiros. Em cada um desses casos, havendo possibilidade de identificação direta ou indireta do titular dos dados, a LGPD se aplica, exigindo proteção apropriada a partir do momento em que os dados são coletados. Exige uma estrutura de privacidade e segurança nos fundamentos de qualquer projeto. Mas, na verdade, os dados mudam ao longo de toda a sua vida útil e muitas vezes são armazenados por anos - seja para registro ou por comodidade. Com a LGPD, no entanto, este último está se tornando um risco e um hábito caro.

8.4.1 Finalidade do GCVD

A Gestão do Ciclo de Vida do Dado (GCVD) é um processo que ajuda as organizações a gerenciar o fluxo de dados em todo o seu ciclo de vida: da criação, uso, compartilhamento, arquivamento e exclusão.

Rastrear dados com precisão em todo o ciclo de vida da informação é a base de uma estratégia de proteção de dados e ajuda a determinar onde aplicar os controles de segurança.

8.4.2 Compreendendo os Fluxos de Dados

Os vários requisitos da LGPD exigem que uma empresa saiba:

- exatamente onde seus dados e, em particular, os dados pessoais se encontram
- para quais finalidades os dados devem ser coletados ou criados
- por quais razões os dados devem ser retidos
- em que prazo ou em que situação os dados devem ser excluídos

8.4.2.1 Coleta de dados

Desde o início, é importante ter em mente quais dados pessoais são necessários para os fins do tratamento pretendido. A LGPD requer um motivo para manter os dados pessoais armazenados; portanto, a qualquer momento, deve ser claro e fácil demonstrar ao menos:

- com que finalidade ou finalidades as informações foram coletadas
- em que momento (inclusive a data) os titulares dos dados foram informados da coleta e da sua finalidade
- se o consentimento foi adquirido para o tratamento pretendido
- em caso positivo, se esse consentimento ainda é válido (e não retirado)
- outro fundamento legal para o tratamento existente

Na prática, cada “pedaço” de informação precisa de numerosas etiquetas indicando porque existe e por quanto tempo continuará existindo.

8.4.2.2 Estrutura das permissões

Qualquer coleta de dados, mas uma coleta de dados pessoais em particular, precisa de uma estrutura de permissões, definindo claramente quais funcionários precisam, por conta de sua função na organização, acessar quais dados pessoais.

No entanto, as coisas mudam. Um bom programa deve avaliar e revisar continuamente quem precisa acessar que tipo ou tipos de informação. Controladores e operadores devem trabalhar com seus colegas de TI para automatizar controles em todos os sistemas corporativos. Eles devem facilitar para que os funcionários façam a coisa certa contra a coisa errada. Eles devem evitar que os funcionários tenham consequências negativas através de suas ações, até mesmo uma simples negligência em fazer alguma coisa.

Depois que a estrutura de permissões estiver em vigor, ela deve ser mantida por meio de avaliações regulares e contínuas.

8.4.2.3 Construir regras de retenção e exclusão

Um dos princípios fundamentais da LGPD é a necessidade, que significa 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 (Artigo 6º, III, LGPD). Na prática, isso leva a um equilíbrio contínuo entre quais dados manter, por qual razão, e quais dados descartar de maneira segura.

Armazenar dados pessoais é um fardo para qualquer organização. É preciso muito esforço para manter os dados seguros, completos e atualizados, e ainda mais esforços para responder às solicitações dos titulares de dados, solicitando informações sobre o tratamento de seus dados e para lidar com reclamações referentes a seus direitos. Adicionalmente, há sempre a ameaça de uma violação de dados pessoais, com os procedimentos resultantes, o risco para os titulares de dados e o risco de dados para a empresa, como perda de reputação, custo de reparações e possíveis multas.

Há muitas obrigações legais em relação à retenção de dados pessoais por um determinado período. Por exemplo, considere-se registros de clientes, como vendas e transações financeiras, garantias ou informações de recursos humanos, como currículo, histórico de pagamento ou informações tributárias.

A boa Gestão do Ciclo de Vida do Dado (GCVD):

- fornece as ferramentas para gerenciar o fluxo de dados em um sistema de informações
- mantém rastreamento dos dados a partir do momento em que são coletados ou gerados até o momento em que são excluídos, porque não há **motivo** para retê-los.

8.5 Auditoria de Proteção de Dados

O artigo 55-J, inciso XVI, da LGPD menciona que a ANPD poderá realizar auditoria sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, para monitorar a conformidade com a LGPD.

Além das auditorias da ANPD, é comum que os próprios agentes de tratamento prevejam em contrato a possibilidade de realização de auditorias, especialmente de um controlador em relação ao operador, para verificação do nível de aderência às previsões contratuais e ao compliance em matéria de proteção de dados pessoais.

8.5.1 Finalidade de uma auditoria

A finalidade de um processo de auditoria de proteção de dados é testar, avaliar e reavaliar regularmente a eficácia de medidas técnicas e administrativas para garantir a conformidade com a LGPD, incluindo a segurança do tratamento.

Normalmente, uma auditoria revelará, por exemplo, **lacunas** nas políticas de privacidade que precisam ser abordadas para aprimorar a governança de privacidade de dados.

No mínimo, uma auditoria tornará a proteção de dados pessoais o "tópico da semana", aumentando a conscientização em toda a organização.

De um modo geral, dois tipos de auditorias de privacidade podem ser distinguidos: uma auditoria de adequação e uma auditoria de conformidade.

8.5.1.1 Auditoria de adequação

Uma auditoria de adequação visa:

- assegurar que haja políticas de proteção de dados adequadas em uma dada organização e que sejam de fato aplicadas a todas as instâncias de tratamento de dados pessoais
    - incluindo conjuntos de dados históricos, backups, equipamentos obsoletos
- avaliar se estas políticas são adequadas para atender aos requisitos da LGPD e outras leis e regulamentos de proteção de dados possivelmente aplicáveis

Isso requer um entendimento e um mapeamento completos dos fluxos de dados em toda a organização, e é mais do que apenas revisar todas as políticas, procedimentos, códigos de conduta e diretrizes da organização que afetam o manuseio de dados pessoais durante seu ciclo de vida. A auditoria de adequação deve ser feita dentro da empresa e com todos os terceiros envolvidos, inclusive operadores.

8.5.1.2 Auditoria de Conformidade

Após a conclusão da auditoria de adequação, a próxima etapa poderá ser, e talvez até deva ser, uma auditoria de conformidade, para determinar se a organização está de fato cumprindo as políticas e procedimentos identificados durante e, talvez, aprimorada como resultado da auditoria de adequação.

Uma auditoria de conformidade requer uma investigação de como os dados pessoais são tratados **na prática** dentro das várias unidades de negócios, entre departamentos e ao lidar com terceiros.

Uma auditoria abrangente de conformidade também deve examinar fatores como:

- se a organização oferece treinamento de conformidade de proteção de dados
- como as políticas de proteção de dados são disseminadas para os funcionários
- como as reclamações de violações de políticas são tratadas

A profundidade da auditoria de conformidade dependerá dos riscos percebidos em relação a infrações legais e envolvendo o tratamento de dados pessoais.

8.5.2 Conteúdo de um plano de auditoria

- Desenvolvimento de programas de auditoria (planejamento)
  - Contatos, finalidades, prazo...
- Descrição da abordagem e o escopo da auditoria:
  - Será uma adequação - ou uma auditoria de conformidade?
  - Auditoria vertical (funcional), visando um departamento específico (como Recursos Humanos) ou
  - Auditoria horizontal (processo); rastreamento de um determinado processo de uma ponta à outra
  - Escopo da auditoria (governança de proteção de dados, gerenciamento de registros, gerenciamento de acesso e segurança de dados, proteção de dados, treinamento e conscientização etc.)
- Preparativos, reunião de evidências das áreas incluídas:
  - Acordos de parcerias
  - Contratos, como de controlador-operador, Normas Corporativas Globais, acordos de divulgação etc.
  - Descrições de processos; ordens de serviço, avisos
  - Material de treinamento, panfletos etc.
- Realização da auditoria
- Relatório:
  - Conclusão geral
  - Áreas de boa prática
  - Áreas para melhoria
- Acompanhamento

8.6 Práticas Relacionadas a Aplicações do Uso de Dados, Marketing e Mídias Sociais

8.6.1 O uso de informações de mídia social em atividades de marketing

Não há muito tempo, havia três métodos de informar ao público sobre o produto ou serviço que um vendedor estava tentando vender:

- comprar publicidade cara
- pedir à mídia para contar sua história
- contratar uma enorme força de vendas para incomodar as pessoas diretamente sobre o produto

Nenhum desses métodos foi realmente muito eficaz. Todos os três métodos foram baseados em interromper as pessoas no que estavam fazendo, esperando que elas pudessem ver o produto e pensar: "é isso o que tenho procurado" e, se assim fosse, então elas se lembrariam de quem anunciava e onde deveriam ir para encontrar esse produto.

Com a internet, existem opções melhores para que seu produto seja notado. Dos produtores e consumidores, as pessoas se tornaram "prosumidores"[5], realizando o design de produtos, criticando e consumindo, gastando dinheiro. Tornou-se fácil criar um site, escrever um blog, publicar conteúdo e mídia (fotos, som, vídeo) nas mídias sociais. Não apenas os fornecedores, mas praticamente todos podem publicar seu próprio conteúdo, que seus consumidores desejam comprar.

[5] para mais informações verifique: https://pt.wikipedia.org/wiki/Prosumer

Com as mídias sociais, todos podem entrar em contato com outras pessoas conectadas a essas mídias sociais, em qualquer lugar do mundo. Só com o Facebook e seus mais de 1,5 bilhão de usuários, um vasto mercado global está aberto.

Com essas mudanças soando na era digital, o negócio está se tornando "multicanal" e interativo. Os fornecedores escrevem sobre seus produtos como jornalistas, e as pessoas reagem a isso indicando que gostam do que veem, gostam do que está sendo produzido, do que está sendo oferecido. Claro, se elas não gostarem, elas não hesitarão em dizer ao mundo sobre isso também - muitas vezes em termos bastante contundentes.

Finalmente, um novo conceito de vendas está surgindo. Muitas pessoas acham importante o que as outras pessoas e, em particular, seus amigos, acham do produto que estão procurando. A mensagem de que "76% dos seus amigos gostam deste produto" prova ser um incentivo para comprar. Mesmo que não haja como verificar essa afirmação, todos parecemos acreditar.

Os consumidores podem ser divididos em grupos com gostos semelhantes, interesses semelhantes e outros grupos relevantes. Ao verificar uma loja on-line, todos nos deparamos com comentários como "compradores do <produto que você acabou de ver> também compraram: <estes outros produtos>". Mensagens como essa provam ser um facilitador de vendas muito forte, desde que o consumidor-alvo tenha gostos e interesses semelhantes aos dos "outros compradores".

8.6.2 Uso da internet no campo do marketing

Para que essa nova economia, mais digital, funcione, as empresas precisam de informações sobre potenciais compradores. Na prática, isso significa que eles precisam de informações sobre o maior número possível de consumidores. Que tipo de consumidor é esse? O tipo "radical", precisando de equipamentos e roupas de boa qualidade para o ar livre? O tipo "eu quero a mais nova tecnologia"? Ou talvez o tipo de melhor relação preço / desempenho, ou melhor, o tipo de comprador que busca o preço mais baixo garantido.

Perfis como esse demandam muitos dados sobre pessoas e seu comportamento. Como essas empresas obtêm essa informação?

8.6.3 Cookies

Um cookie é apenas um arquivo de texto (geralmente pequeno), armazenado no computador do usuário. Os cookies mais comuns são:

- cookies de sessão
- cookies persistentes
- cookies de rastreamento

8.6.3.1 Cookies de sessão

Os cookies de sessão permitem que os usuários sejam reconhecidos dentro de um site, de modo que qualquer alteração de página ou seleção de item ou de dados que o usuário faça seja lembrada de uma página para outra. O exemplo mais comum é o recurso de carrinho de compras de qualquer loja virtual. Sempre que os itens são selecionados, a seleção é armazenada no cookie da sessão, por isso é lembrada até que o usuário esteja pronto para fazer check-out.

Ao fazer logon em um site, um cookie de sessão na memória do computador do usuário retém as informações de que o logon foi bem-sucedido, pois o site não tem como lembrar que você fez logon. Ao sair do site, o que usualmente significa fechar o navegador, o cookie da sessão é apagado da memória do computador do usuário e, como resultado, ele é desconectado.

8.6.3.2 Cookies persistentes

Os cookies persistentes permanecem no disco rígido do usuário até serem apagados pelo usuário ou até expirarem. Os cookies persistentes podem oferecer serviços simples ao usuário como visitante recorrente. Por exemplo, para manter a seleção de idioma do usuário. Quando o usuário revisitar esse site, ele oferecerá, com base nas informações do cookie, o conteúdo no idioma escolhido durante a visita anterior.

Esse tipo de cookie pode tornar a experiência do visitante do site mais pessoal. Por exemplo, um usuário usa um site de reservas para reservar um voo barato para a Inglaterra. Para que as transações (financeiras e com a companhia aérea) sejam bem-sucedidas, o usuário deve preencher informações pessoais (nome, endereço, número do passaporte, detalhes do cartão de crédito). Na próxima vez que o usuário visitar o site, a combinação dessas informações poderá levar a uma saudação mais pessoal, como "Bom dia, <nome>", mas também a ofertas de outras viagens, seguro de viagem, ofertas de bons equipamentos para caminhadas, malas de viagem, e mais. Tudo com base nas informações coletadas da viagem reservada e, se aplicável, nas viagens reservadas anteriormente.

Não há necessidade de salvar informações no cookie. De fato, um identificador único é suficiente para reconhecer o usuário (ou pelo menos seu dispositivo ou browser) e vincular esse identificador a um banco de dados.

8.6.3.3 Cookies de rastreamento

Um cookie de rastreamento geralmente é chamado de cookie de terceiros. Ele é colocado no disco rígido de um usuário por um site de um domínio diferente daquele que o usuário está visitando.

Assim como acontece com os cookies padrão, os cookies de terceiros colocados no computador do usuário possibilitam salvar algumas informações sobre o usuário para uso posterior. Entretanto, os cookies de terceiros, são geralmente definidos por redes de publicidade nas quais um site pode se inscrever.

O objetivo dos cookies é acompanhar quais páginas uma pessoa está visitando, construindo um perfil da pessoa com base em interesses. O perfil pode ser adicionado usando informações de outros sites em sua rede. Ele não está vinculado a detalhes pessoais conhecidos do site, mas apenas exibe anúncios ao perfil do usuário para que eles sejam os mais relevantes possível.

8.6.4 Outras informações de perfil: o preço dos serviços "gratuitos"

O Facebook e o Google sabem quase tudo o que há para saber sobre os usuários de seus produtos gratuitos.

> Coletamos o conteúdo e outras informações que você fornece ao usar nossos serviços, inclusive quando você se inscreve em uma conta, cria ou compartilha e envia mensagens ou se comunica com outras pessoas. Isso pode incluir informações no ou sobre o conteúdo que você fornece, como a localização de uma foto ou a data em que um arquivo foi criado. Também coletamos informações sobre como você usa nossos serviços, como os tipos de conteúdo visualizados ou envolvidos, ou a frequência e duração de suas atividades.
>
> Fonte: Política de Privacidade do Facebook

O mesmo vale para o Google. Com seu mecanismo de pesquisa usado por bilhões de pessoas, combinado com informações do LinkedIn, mapas do Google e postagens de blog, o Google sabe quais pessoas estão pesquisando ou comprando ativamente e quais palavras ou frases elas usam para encontrá-las. Eles sabem para cada um de seus usuários o que provavelmente comprarão em breve, o que precisarão comprar agora, mais tarde hoje, amanhã e muito mais.

O Google sabe isso e muito mais devido às informações que detém sobre onde estamos, quem somos, onde estaremos e o que faremos. Eles sabem quem somos, quanto gastamos, o que fazemos para viver, nossos dados demográficos (idade, sexo, religião, renda, educação), onde moramos, quem são nossos amigos, o que fazemos fora do trabalho, em quem votamos, em que televisão, podcasts, música ou outro entretenimento que consumimos, além de diversas outras informações.

O Google também sabe como todas essas coisas mudaram ao longo do tempo. Isso lhe permite encontrar tendências e prever o comportamento, tanto no nível individual quanto no agregado. Em resumo, ele tem exatamente as informações que as empresas precisam para maximizar seu marketing. Essas também são as informações necessárias para fornecer o produto ou serviço que você precisa, exatamente no momento em que você precisa.

8.6.5 Perspectiva de proteção de dados

A LGPD não impede a inovação e o tratamento de dados pessoais – apenas determina princípios, bases legais e outros parâmetros e limites para que essas operações ocorram de modo sustentável a longo prazo, sem que causem riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais.

8.6.5.1 Cookies

Os cookies de sessão normalmente são necessários para efetuar a transmissão de uma comunicação eletrônica através de uma rede de comunicações eletrônicas, ou para fornecer um serviço da sociedade da informação requerido pelo utilizador final, ou ainda para a medição do público na web, desde que essa medição seja efetuada pelo fornecedor do serviço da sociedade da informação solicitado pelo utilizador final. Para cumprir tais finalidades, podem ser armazenados sem o consentimento expresso do usuário, como no carrinho de compras on-line discutido anteriormente.

Para outros cookies, é necessário o consentimento nos moldes definidos pela LGPD. Esse consentimento deve ser livre, informado e inequívoco. A novidade da vez (e que tem sido bastante utilizada) é que os usuários finais podem expressar o consentimento (ou retirá-lo) facilmente pelas configurações do navegador. Isso ajuda a minimizar a sobrecarga de banners e pop-ups.

8.6.5.2 Criação de Perfil

Não há dúvida de que a LGPD se aplica à criação de perfil, conforme descrito no Artigo 20. Por conseguinte, o titular dos dados tem o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

No mesmo dispositivo, a LGPD ainda determina que:

> O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
>
> Em caso de não oferecimento de informações de que trata o [parágrafo anterior] baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.
>
> Fonte: Lei Geral de Proteção de Dados (LGPD), Lei n.13.709/2018 (art. 20, §§ 1º e 2º)

Mas ainda há muitos serviços "gratuitos", oferecendo conteúdo ou outros produtos ou serviços gratuitos, desde que o usuário autorize a coleta de informações sobre ele, seus interesses e gostos para "selecionar propaganda apropriada". A LGPD não mudará isso, mas pelo menos nos

dará a chance de realizar essa operação de modo mais consciente e com proteção dos dados pessoais.

Cabe ao titular dos dados ter cuidado com as informações reveladas às empresas que oferecem serviços gratuitos. O ponto é que a maioria das pessoas está acostumada a concordar com declarações longas sem realmente lê-las. A LGPD proíbe a declaração longa e ilegível e requer uma linguagem simples e clara, explicando para qual finalidade os dados pessoais coletados devem ser usados.

8.7 Big data

O tratamento atual de grandes quantidades de informações de pessoas para a criação de perfis traz um grande desafio. O desafio é justamente encontrar um equilíbrio entre as preocupações com a proteção da privacidade e das liberdades pessoais e a possibilidade de apoiar o desenvolvimento econômico e tecnológico e a inovação com o uso dos dados.

E não são apenas as organizações que desejam que os dados sejam utilizados – os próprios titulares demandam esse tipo tratamento para a entrega de valor e conveniência a si próprio! A personalização facilita uma série de atividades e faz com que o titular se sinta especial com determinadas customizações.

É necessário que essa entrega de valor e conveniência seja acompanhada de uma preocupação atenta para que se evitem, no tratamento dos dados pessoais, problemas como a discriminação, a manipulação e supressão de direitos e liberdades fundamentais, a vigilância e repressão, e o cometimento de crimes decorrentes do acesso indevido às informações pessoais.

Se conseguirmos garantir que os dados pessoais serão tratados da forma correta (de acordo com a legislação) e em benefício (direto ou indireto) dos próprios titulares, por exemplo, estaremos no caminho certo.

Contato EXIN

www.exin.com