A proteção de dados pessoais e as Organizações da Sociedade Civil: uma questão de Direitos Humanos

Organização: Fátima Nascimento

ELO LIGAÇÃO E ORGANIZAÇÃO
Brot für die Welt
Abong

O ELO Ligação e Organização é uma associação civil fundada em 1996, com sede na cidade de Salvador – Bahia. Seu corpo associativo é composto por profissionais vinculados a diversos movimentos sociais e universidades, e consultores independentes que têm em sua origem o trabalho em organizações da sociedade civil, organizações ecumênicas e agências de cooperação internacional.

O trabalho do ELO é dirigido a organizações da sociedade civil de diferentes portes, movimentos sociais, associações comunitárias urbanas e rurais, cooperativas populares, além de organizações nacionais e internacionais que apoiam projetos de desenvolvimento social no Brasil.

A proteção de dados pessoais e as Organizações da Sociedade Civil: uma questão de Direitos Humanos

Organização:

FÁTIMA NASCIMENTO

Textos:

Fátima Nascimento; Aline Viotto e Laura Arantes; Maraísa Rosa Cezarino; Manoel Nascimento.

Salvador, dezembro de 2025

Índice

Apresentação

O texto ora compartilhado busca discutir o porquê de uma Lei Geral de Proteção de Dados Pessoais (LGPD) e a sua importância para as nossas vidas, nossas organizações e na garantia dos Direitos Humanos.

A LGPD é parte de um movimento mundial e traz um grande avanço no sentido de assegurar a proteção de dados de pessoas físicas, diante de cada vez mais solicitações de dados pessoais (compras, acesso a sites de pesquisa, aplicativos de serviços, na participação em eventos presenciais ou virtuais etc.), sem que, na maioria das vezes, fique nítido como as informações fornecidas serão utilizadas. Nós mesmos, enquanto Organizações da Sociedade Civil (OSC), necessitamos apresentar aos nossos apoiadores listas de presença com dados de participantes das atividades realizadas pelos projetos, disponibilizamos depoimentos (áudios/vídeos) em formatos diversos (e em mídias abertas: sites, redes sociais), coletamos informações pessoais de prestadores de serviço e colaboradores, para mencionar alguns exemplos. Se nossa ação consiste em prestação de serviço nas áreas de saúde, educação, ação social, regularização fundiária etc.; ou se trabalhamos com alguns perfis populacionais como criança e adolescentes, LGBTQIAP+, entre outros, os cuidados com o uso e o armazenamento dos dados devem ter ainda mais camadas de segurança, como forma de evitar que informações sensíveis (prontuários de saúde, por exemplo) sejam expostas e prejudiquem tanto a pessoa titular do dado quanto o trabalho realizado pela organização, e ainda pode incidir em multa para a instituição pelo descuido com o tratamento e guarda dos dados a ela confiados.

Com o objetivo de tornar a LGPD acessível às OSCs, o ELO preparou e ofereceu um curso em formato EAD sobre o tema com turmas que foram formadas nos anos de 2023 e 2024. O documento que segue é a compilação dos textos disponibilizados no curso. Com esta publicação esperamos:

1) Informar o motivo de uma Lei Geral de Proteção de Dados Pessoais, seus principais conceitos, princípios e medidas de proteção, bem como as sanções no caso de violação da LGPD;

2) Contribuir para a adoção de políticas e medidas institucionais que garantam a proteção de dados pessoais que são coletados, tratados, compartilhados nas e pelas OSCs;

3) Sensibilizar as OSCs para a importância da proteção de dados pessoais como elemento fundamental da luta pelos direitos humanos.

Equipe ELO

I. A LGPD e as Organizações da Sociedade Civil: uma breve introdução

Fátima Nascimento[1]

[1] Advogada, mestre em Políticas Sociais e Cidadania, Consultora associada do Elo e assessora de Organizações da Sociedade Civil.

Este texto apresenta os antecedentes e pressupostos da Lei Geral de Proteção de Dados, sua implementação e a necessária adequação das Organizações da Sociedade Civil (OSC), tais como associações sem finalidade lucrativa, fundações e institutos.

A Lei Geral de Proteção de Dados, conhecida pela sigla LGPD, Lei nº 13.709/2018, entrou em vigor em agosto de 2020, com a Autoridade Nacional de Proteção de Dados (ANPD) - agência responsável pela fiscalização da aplicação da Lei, sendo instituída neste mesmo ano.

A LGPD é parte de um movimento internacional de proteção de dados pessoais em face à ampliação da disponibilização de informações no ambiente virtual, seja para fins de acesso a serviços públicos ou privados, para compras etc., seja para a transformação destes em dados para uso com fins diversos (desenvolvimento de produtos, campanhas eleitorais etc.); e **tem como finalidade estabelecer e garantir os direitos de todas as pessoas que fornecem dados pessoais para acessar produtos e serviços, determinando quando, como e por que os dados podem ser tratados, armazenados, compartilhados e eliminados tanto pelo governo como também pelas empresas e pelas organizações da sociedade civil**.

Origem e Conceito

A informática, a automação do processo produtivo, o desenvolvimento da internet e os constantes avanços tecnológicos decorrentes trouxeram mudanças significativas em nossas vidas e na forma como nos relacionamos. Essas mudanças têm gerado a necessidade de regulação das relações estabelecidas de forma a proteger as pessoas do uso indevido de seus **dados pessoais**, sendo estes considerados como **toda e qualquer informação que identifique ou possa identificar uma pessoa**.

O conceito de proteção de dados pessoais teve origem na Europa, ainda nos anos de 1970, como decorrência do avanço da informatização e automação dos setores público e privado e foi **consolidado como sendo a capacidade de cada pessoa determinar de forma autônoma como seus dados pessoais podem ser utilizados por terceiros com base em uma série de garantias que evitem que esses dados sejam utilizados de forma discriminatória ou que possam causar danos para si ou para a coletividade.**

As primeiras legislações a respeito da proteção de dados pessoais

A primeira legislação direcionada ao tema da proteção de dados pessoais de que se tem notícia foi criada e implementada no estado de Hesse, na Alemanha, no ano de 1970.

Em 1977, a Alemanha implantou a sua lei federal, seguida de países como Áustria, França, Noruega e Suécia, que criaram suas próprias leis em 1978. Uma convenção do então Conselho da Europa, realizada em 1981, ajudou a unificar e melhorar o tratamento automatizado de dados pessoais. Na Europa, a normatização continuou sendo aperfeiçoada com a promulgação da Diretiva 95/46/CE da União Europeia, que determinava que cada país-membro adequasse suas legislações e estabelecesse um órgão ou profissional responsável pela supervisão e implementação da lei.

Todas essas leis seguem os princípios básicos estabelecidos na Lei de Hesse, quais sejam: (i) o recolhimento, armazenamento e utilização de dados pessoais só podem ocorrer com a autorização do titular e (ii) devem ser coletados diretamente junto ao titular; (iii) os dados não devem ser mantidos por muito tempo e excluídos após período apropriado; (iv) minimização de dados; (v) limitação de finalidade, em que o processamento de dados é permitido somente para propósito específico previamente definido; (vi) transparência; (vii) necessidade, quando não há outras formas disponíveis.

A transnacionalização das empresas levou também à transferência de dados entre diferentes países. Para regular a transferência de dados pessoais entre Estados Unidos e Europa foi firmado o acordo *Safe Harbor*, assinado em 2000. Em 2015 o acordo foi revogado por suspeitas de espionagem por parte da Agência de Segurança Nacional dos EUA. Porém, já no ano seguinte, a Europa aprovou um novo programa de transferência internacional de dados, conhecido como *Privacy Shield*, possibilitando aos cidadãos e cidadãs europeias maior segurança no uso de dados por empresas norte-americanas.

Finalmente, como resposta aos grandes casos de vazamento de dados, referente à utilização, ao comércio e à exportação de dados pessoais, no ano de 2018 foi estabelecido o Regulamento Geral sobre a Proteção de Dados (GDPR 2016/679).

> "O GDPR obrigou empresas de todo o mundo – inclusive gigantes como o Facebook e o Google – a mudar a forma como coletam e tratam dados e foi responsável por uma onda de novas leis sobre o tema em todo o mundo, inclusive no Brasil."[2]

A consolidação de mecanismos de proteção de dados pessoais no Brasil

No Brasil, a Lei Geral de Proteção de Dados foi aprovada em 2018 e entrou em vigor em agosto de 2020. A Lei brasileira tem influência da GDPR europeia. Porém, o tema da garantia da privacidade não é exatamente recente. A Constituição de 1988, em seu artigo 5º, estabelece os direitos e deveres dos/as cidadãos/ãs, mesmo que de maneira genérica. Trata no inciso X da privacidade, ao dizer que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Em 1993, a aprovação do Código de Defesa do Consumidor aprofunda a defesa da informação e introduz uma seção específica sobre cadastros e bancos de dados, garantindo ao cidadão/ã consumidor/a o acesso e a correção de seus dados que estejam à disposição de alguma empresa, além da garantia de privacidade e responsabilização das empresas quanto à segurança dos dados. "*Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para fins de atendimento*". O decreto nº 7.962/2013 complementou o Código de Defesa do Consumidor, definindo como diretrizes do Plano Nacional de Consumo e Cidadania a "*autodeterminação, privacidade, confidencialidade e segurança das informações e dados pessoais prestados ou coletados, inclusive por meio eletrônico" (*artigo 2º.).

Em 1996, também em relação à privacidade, uma nova lei (Lei 9.296/96) acrescentou que é "inviolável o sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Mas o caminho para a LGPD foi pavimentado mesmo pela mobilização de muitos setores da sociedade civil, especialmente das organizações, grupos, redes e articulações que se ocupam dos direitos em tempos de internet, e que levou à proposição, discussão e aprovação do Marco Civil da Internet, consolidado pela Lei 12.965/2014.

[2] História das leis de proteção de dados e privacidade na internet, em http://assismendes.com.br.

Em seu artigo 3º, o Marco Civil da Internet determina que o uso da Internet tem como princípios, dentre outros, a proteção da privacidade (inciso II), a proteção dos dados pessoais (inciso III) e a responsabilização dos agentes de acordo com suas atividades (inciso VI). Conceitos como o de neutralidade de rede e o da liberdade de expressão foram introduzidos, assim como foram definidas as obrigações dos órgãos públicos quanto ao fornecimento da internet.

E, mais recentemente (2022), por meio de uma emenda constitucional (115/2022), a proteção de dados pessoais tornou-se um direito fundamental[3] previsto na Constituição Brasileira, como inciso LXXIX do artigo 5º. da CF.

A LGPD e as Organizações da Sociedade Civil

A LGPD tem entre seus principais pontos: o direito da pessoa titular acessar, atualizar, corrigir e solicitar a exclusão de seus dados; um maior cuidado com dados sensíveis; a portabilidade dos dados; as sanções administrativas e jurídicas quando do descumprimento da Lei, promovendo assim maior transparência e tranquilidade quanto à privacidade dos dados pessoais.

A nova Lei de proteção de dados pessoais se aplica a todas as instituições e pessoas que tratam dados pessoais, consequentemente, também deve ser observada pelas organizações da sociedade civil que coletam e tratam informações pessoais na execução de seu trabalho, sejam elas dados de pessoas beneficiárias, colaboradores/as, parceiros/as e fornecedores, de forma física e digital, e que são utilizados para o atendimento direto ao público, para a realização de atividades formativas, de articulação, publicações e campanhas, na captação de recursos e prestações de contas de recursos etc., enfim, no desenvolvimento de suas ações.

A adequação à LGPD é uma forma efetiva de colaborar para a construção de uma cultura de proteção de dados pessoais entre aquelas pessoas com as quais a OSC trabalha e se relaciona por meio da sensibilização e formação para esta questão, e de maneira mais ampla, de somar forças junto àqueles/as que trabalham no constante aprimoramento das normatizações para o terceiro setor. E, por fim, de colaborar para que pessoas que fornecem seus dados não venham a sofrer algum tipo de dano, seja a sua pessoa, seja a seu grupo e/ou comunidade.

[3] Emenda Constitucional 115/2022.

II. Fique por dentro da LGPD: perguntas e respostas sobre os principais conceitos da Lei Geral de Proteção de Dados Pessoais

Aline Viotto e Laura Arantes[4]

[4]Aline Viotto é mestre em Direito Econômico pela Faculdade de Direito da Universidade de São Paulo (USP). Laura Arantes é graduada em Direito pela USP, ambas atuam na VMCA Advogados, na área de terceiro setor e negócios de impacto.

1. **Para que uma lei geral de proteção de dados?**

A Lei Geral de Proteção de Dados Pessoais - LGPD - foi aprovada em 2018 com a função dual de regulamentar o uso de dados pessoais e fomentar a inovação. Seu principal objetivo é garantir a proteção à privacidade e à inviolabilidade da honra, da imagem e da intimidade dos cidadãos brasileiros, ao mesmo tempo em que permite a exploração econômica no setor, por meio de regras específicas para o tratamento de dados pessoais, seja coleta, transferência, classificação ou utilização. Trata-se de fruto de uma longa discussão, iniciada em meados de 2010, que resultou em um texto normativo elaborado por muitos setores, tanto do governo quanto da academia, da sociedade civil e do setor privado.

Com isso, a LGPD pode ser considerada um pilar fundamental para a concretização do arcabouço normativo da **proteção de dados pessoais e para a segurança jurídica dos titulares de dados – e não um mecanismo de impedimento do manuseio dessas informações**. Assim, guiadas pelos princípios da Constituição Federal, da LGPD e das demais disposições normativas aplicáveis, as Organizações da Sociedade Civil (OSC) devem voltar sua atenção aos processos internos relacionados ao cumprimento dessas exigências legais.

Com inúmeros casos de vazamento de dados relatados em período recente, uma das maiores preocupações relacionadas à proteção de dados é quanto às consequências desse tipo de incidente. Acerca da realidade das OSCs, ainda há um certo desconhecimento sobre o que exige a LGPD e diversas dificuldades para se adequar a ela, na medida em que muitas entidades não possuem recursos suficientes para rever seus procedimentos, elaborar políticas de privacidade, treinar suas equipes, realizar as inúmeras etapas do processo de adequação à Lei e dispor da tecnologia necessária para proteção de seus bancos de dados. **Apesar dos desafios, é importante que as OSCs adotem medidas que garantam o cumprimento das exigências legais na execução de suas atividades e que sejam atores ativos na difusão da cultura de proteção aos dados pessoais, reforçando assim a relação de confiança da sociedade nas organizações.**

Dessa forma, este texto tem como objetivo apresentar pontos relevantes da proteção de dados pessoais no contexto das atividades desempenhadas pelas OSCs, por meio do modelo de perguntas e respostas, sobre a necessidade dessas em se adaptarem à LGPD e sobre as principais dúvidas atinentes a esse tema.

2. O que a LGPD visa proteger? Qual a diferença entre dados pessoais e dados pessoais sensíveis?

A Lei consolida no Brasil a ideia de que os dados pessoais de um indivíduo devem ser protegidos pela legislação, ou seja, trata-se de um bem jurídico a ser tutelado. Em vista disso, busca-se não somente provocar uma mudança na cultura de tratamento de dados, como lapidar os contornos referentes às responsabilidades e competências dessa atividade.

A Lei se aplica a qualquer tratamento de dado pessoal por pessoa física ou jurídica, de direito público ou privado, com ou sem fins lucrativos. Logo, toda organização que capta e armazena dado pessoal precisa estar adequada ao que exige a LGPD. Por esse motivo, a Autoridade Nacional de Proteção de Dados - ANPD - vem gradativamente voltando sua atenção para os agentes de pequeno porte, incluindo nesse rol aqueles que não possuem finalidade lucrativa, e discutindo com a sociedade alternativas para flexibilizar os critérios de cumprimento da Lei para esse grupo.

O texto normativo é respaldado por alguns princípios (finalidade, necessidade, não discriminação, entre outros) que visam a coordenar essas atividades de tratamento, de forma a afastar a ideia de que os dados pessoais possam ser considerados apenas como uma "moeda de troca" em uma relação econômica.

Mas o que exatamente significa tratar um dado pessoal? A Lei dispõe que é toda e qualquer operação realizada com o dado pessoal, desde o momento em que ele entra no banco de dados até ser excluído. Inclui, entre outras operações, a coleta, produção, recepção, utilização, transmissão, armazenamento, modificação ou exclusão de dados pessoais. Dentre as atividades de tratamento, também pode-se conceituar anonimização, que aparece algumas vezes na LGPD, e pseudonimização.

A anonimização é um procedimento por meio do qual a ligação entre o/a titular do dado pessoal e as informações sobre ele/a é quebrada, impedindo a identificação. Deve ser considerada a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento do dado no processo de anonimização. No caso dos dados anonimizados, não se aplica a LGPD por não se tratar de informação relacionada à pessoa natural identificada ou identificável. Já a pseudonimização é um procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Diferentemente dos dados anonimizados, os dados pseudonimizados são dados pessoais e estão submetidos ao regime da LGPD.

Tendo em vista essas definições, é importante que as organizações tenham ciência de dois conceitos básicos para entender quando deve ser aplicada a LGPD. O primeiro é a definição de **dado pessoal**, que se refere à "informação relacionada à pessoa natural identificada ou identificável", nos termos do art. 5º, I, da Lei. Em outras palavras, **trata-se de qualquer informação que seja ou possa ser conectada a um indivíduo específico. Alguns exemplos são comuns: nome, CPF, RG e filiação.**

É importante ressaltar que, por definição, a LGPD busca proteger o direito à proteção de dados atinente a uma pessoa física, não contemplando em seu escopo as informações referentes a pessoas jurídicas, a menos que essas últimas revelem informações sobre uma pessoa física (como, por exemplo, no caso de empresários individuais). É importante também destacar que essa definição é sempre contextual, ou seja, há muitas informações que podem ou não ser consideradas como dados pessoais, a depender de quem tem acesso a elas e quais outras informações essa pessoa possui. Como exemplo podemos citar o número de matrícula de um estudante: o número de identificação em si pode não ser considerado um dado pessoal, em razão da impossibilidade de relacioná-lo, fora de um contexto específico, com uma pessoa natural. Todavia, esse número de matrícula, quando combinado com uma base de dados que contenha o nome dos/as estudantes da respectiva escola, pode passar a ser considerado um dado pessoal.

Por outro lado, a Lei define quais são os **dados pessoais** considerados **sensíveis**. Nos termos do art. 5º, II, referem-se ao "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Nota-se, assim, que se trata de uma categoria mais específica de informações, relacionadas ao foro íntimo do indivíduo, e que, por essa razão, apresenta um rol mais enxuto das bases legais de tratamento que podem ser aplicadas e uma série de salvaguardas que devem estar presentes no tratamento.

Assim, é possível entender que a principal diferença entre essas duas categorias de dados pessoais é o regime de proteção atribuído, se mais flexível ou mais restritivo, refletindo nos procedimentos que devem ser adotados pelas organizações para garantir a legalidade do tratamento.

3. Como saber qual agente de tratamento eu sou? Quais são minhas responsabilidades e obrigações em cada caso?

A LGPD define como agentes de tratamento o controlador, o operador e o encarregado (ou DPO - PHP Data Object), que são detentores de diferentes níveis de responsabilidades com relação às atividades de tratamento de dados pessoais. De forma geral, pode-se dizer que o controlador, o qual pode ser uma pessoa física ou jurídica, é que possui poder de mando sobre o tratamento de dados pessoais, ou seja, é ele quem decide os caminhos e diretrizes para o tratamento de uma base de dados específica. É o controlador que tem poder sobre os elementos essenciais das atividades de tratamento, quais sejam, a finalidade, a definição da base legal, o período de armazenamento dos dados, a garantia dos direitos dos titulares, a definição dos dados e dos indivíduos envolvidos na operação de tratamento, entre outras responsabilidades.

Como efeito, é de suma importância que as organizações mapeiem as atividades de tratamento que realizam dentro da entidade e atribuam razões específicas para a ocorrência de cada uma, para compreender de forma nítida em que enquadramento se encontram enquanto agentes de tratamento. Assim, nas atividades em que figurar como controladora do tratamento, ou seja, nos tratamentos em que tiver poder decisório sobre os aspectos mencionados acima, a organização poderá tomar as medidas cabíveis, como, por exemplo, identificar a base legal adequada para respaldar as operações de tratamento. Além disso, dentre outras obrigações previstas na Lei, deverá o controlador informar a finalidade do tratamento de forma detalhada ao titular e garantir que seu uso futuro seja compatível com o propósito previamente comunicado.

Por outro lado, o operador será o agente, pessoa física ou jurídica, que realiza o tratamento de dados pessoais em nome de um controlador. Ou seja, o controlador passa a delegar uma parcela da atividade de manuseio dos dados a um terceiro, que irá tratá-los com base nos interesses estipulados pelo primeiro. É importante refletir que o operador, de forma diferente do que possa parecer, não é necessariamente um subordinado da parte controladora. Isso porque cabe ao operador decidir, por exemplo, quais métodos tecnológicos utilizar para a coleta dos dados, como irá armazenar esses dados, quais as medidas de segurança que irá utilizar, quais os métodos de transferência para o caso de compartilhamento com terceiros envolvidos, quais os meios de recuperação de dados, entre outros critérios. Apesar de não subordinado, o operador deverá restringir a sua atuação aos limites impostos pelo controlador, seguindo todas as orientações que forem dadas por este, desde que sejam lícitas.

O encarregado pelo tratamento de dados pessoais, por sua vez, é o responsável pelo contato com os titulares de dados e pela interface com a ANPD (art. 5º, VIII e 41). Compete a ele responder por eventuais questionamentos, dúvidas e exigências formuladas pelo titular. Por isso, a LGPD prevê que o controlador deve indicar e divulgar publicamente, de preferência em seu site, as informações de contato do encarregado.

É importante que, independentemente da posição ocupada, as organizações estabeleçam instrumentos jurídicos específicos com os agentes envolvidos no tratamento em referência, a fim de realizar um manejo dos riscos, delimitar os papéis enquanto agentes de tratamento e limitar a responsabilidade de cada parte. Apesar de não ser uma obrigação prevista expressamente na LGPD, considera-se uma boa prática a adoção de cláusulas específicas para a proteção de dados pessoais, não somente para comprovar perante terceiros (a exemplo de financiadores) que sua entidade está em processo de adaptação à LGPD, mas também para delimitar as diretrizes para o tratamento que o controlador pretende transmitir ao operador. No final, embora esses papéis sejam definidos por meio de instrumentos contratuais, prepondera a realidade fática. Assim, ainda que um documento diga que a parte A é operadora e a parte B é controladora, o caso concreto sempre prepondera na definição de qual posição, de fato, a entidade está ocupando.

É importante ressaltar que as figuras de operador e controlador não devem ser atreladas a funcionários ou colaboradores específicos que estejam agindo em nome e de forma subordinada ao agente.

4. Quais são as bases legais de tratamento de dados pessoais?

Se está claro que estamos falando de um dado pessoal, o próximo passo é saber se há autorização para tratá-lo, ou seja, é preciso elucidar se existe uma justificativa na lei ("base legal") para aquele tratamento. A LGPD apresenta dez hipóteses em que é possível o tratamento de dado pessoal. A base legal mais comum e mais conhecida é (1) o consentimento, uma autorização expressa do titular de dados pessoais para que seus dados sejam utilizados para determinada finalidade.

O tratamento de dados pessoais será possível quando realizado para: (2) o cumprimento de obrigação legal ou regulatória pelo controlador, (3) o exercício regular de direitos em processo judicial, administrativo ou arbitral e (4) a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular. Além disso, temos a hipótese de tratamento de dados pessoais pela (5) administração pública, quando os dados forem necessários para a execução de políticas públicas. A Lei também prevê a possibilidade de tratamento para (6) realização de estudos por órgãos de pesquisa, (7) em casos para assegurar a proteção da vida ou da incolumidade física do titular ou de terceiros, (8) em situações que envolvam procedimentos realizados por profissionais da área da saúde ou por entidades sanitárias e de (9) proteção ao crédito.

Por fim, a Lei prevê ainda a base legal (10) do legítimo interesse, a qual possibilita o tratamento do dado pessoal sem consentimento quando, a partir de um balanceamento dos interesses em jogo, verifica-se que o interesse da entidade responsável pelo tratamento é legítimo e não gera danos relevantes aos direitos dos titulares de dados pessoais. É importante ressaltar que o instituto do legítimo interesse deve ser empregado com cautela, pois dependerá de análise fundamentada e casuística. Para aplicação dessa base legal, a análise envolverá a natureza do dado, a forma como está sendo processado e a adoção de salvaguardas de segurança pelo controlador.

No âmbito de parcerias com o poder público, a OSC por vezes pode vir a receber um conjunto de dados pessoais para o cumprimento de suas funções. Nesse caso, em que a OSC atua como operadora, ela não é responsável por identificar quais as bases legais que os referidos órgãos da Administração Pública empregam para o tratamento de dados pessoais. De toda forma, ao desenvolver suas atividades, as OSCs devem certificar-se que os dados pessoais serão tratados somente para as finalidades associadas à parceria.

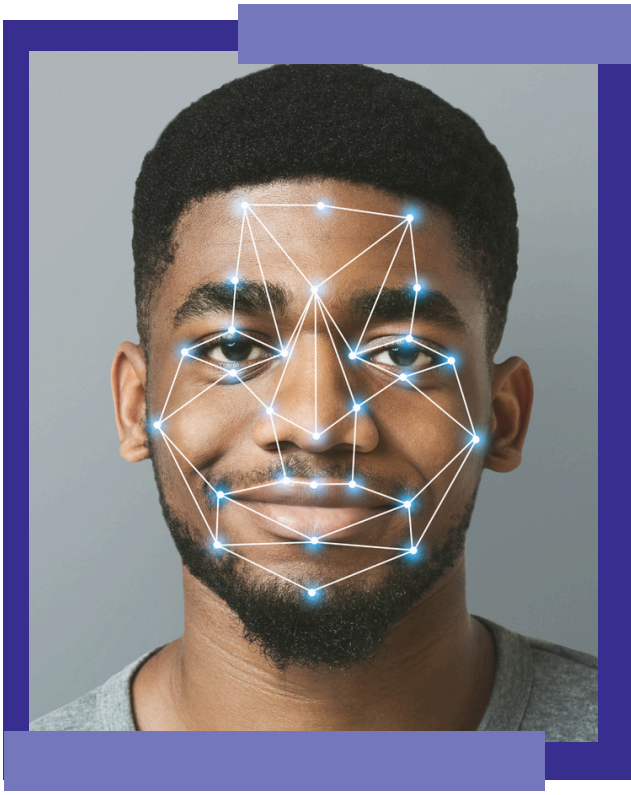
No caso de outros processamentos de dados pessoais iniciados pela própria OSC, em que essa atuará como controladora dos dados pessoais, será necessária a identificação de base legal válida para o tratamento.

5. Quais são os princípios da LGPD?

Além dos direitos dos titulares de dados pessoais, a OSC também deve sempre se atentar ao cumprimento dos princípios de tratamento de dados pessoais. Nesse sentido, o tratamento de dados deverá ter sempre uma finalidade legítima, devidamente informada ao titular dos dados; além disso, é importante que esse tratamento esteja adequado àquilo que foi efetivamente informado ao titular e que ele ocorra na medida necessária para atingir essa finalidade.

A LGPD incorpora também os princípios da segurança e prevenção. Esses orientam que as entidades adotem medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas relacionadas aos dados pessoais, bem como da ocorrência de outros danos decorrentes do tratamento. Nesse mesmo sentido, o princípio da responsabilização e prestação de contas obriga o responsável pelo tratamento dos dados pessoais a demonstrar de forma transparente a adoção de medidas eficazes e capazes de garantir o cumprimento das normas de proteção de dados pessoais.

Por fim, o princípio da não discriminação também é um ponto importante da LGPD. Esse princípio estabelece, ainda que de forma aberta, a impossibilidade de realização de tratamento para fins discriminatórios, ilícitos ou abusivos. Existe outra previsão da norma, entretanto, que dá maior concretude a esse princípio: trata-se da previsão do direito do titular em obter uma revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. Um dos objetivos dessa norma é garantir que não existam aspectos discriminatórios em tratamento automatizado de dados pessoais.

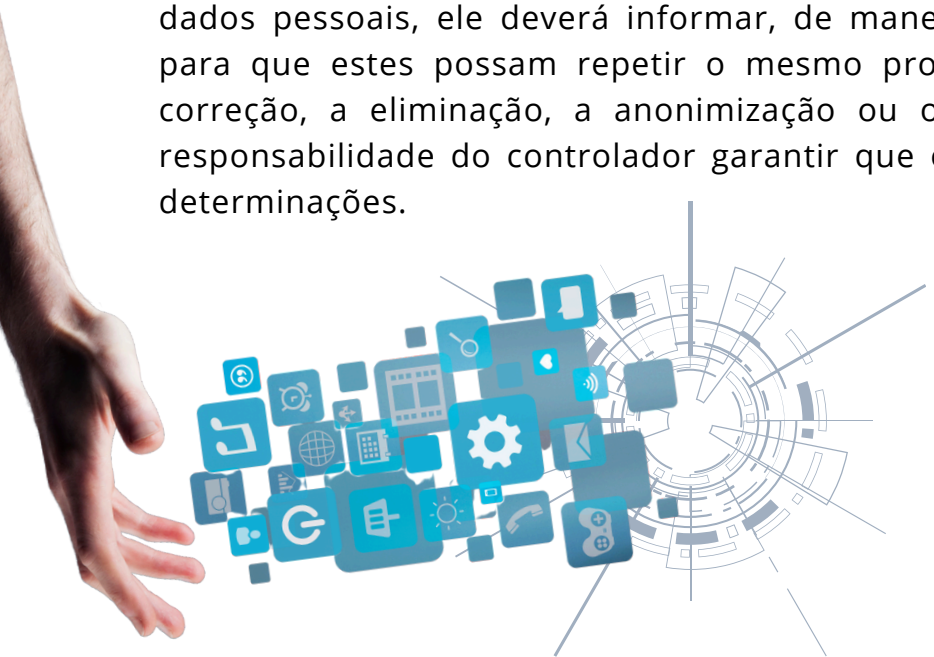


6. Quais são os direitos dos titulares de dados pessoais?

Os titulares de dados pessoais têm uma série de direitos que deverão ser cumpridos pelo controlador de dados pessoais. São eles:

- Direito a ter informações sobre como seus dados são tratados;
- Direito de acesso aos dados: o titular pode requisitar cópia dos seus dados pessoais armazenados pelas entidades;
- Direito de retificação de dados incompletos, inexatos ou desatualizados;
- Direito de requisitar eliminação ou anonimização de dados desnecessários ou excessivos;
- Direito de ser informado sobre o compartilhamento dos seus dados com entidades públicas e privadas;
- Direito de eliminação: o titular pode solicitar a eliminação de seus dados tratados com base no consentimento;
- Direito de ser informado sobre as possibilidades e as consequências de não fornecer o consentimento, quando esse for a base legal de tratamento;
- Direito de revogar o consentimento dado à organização para tratamento de dados pessoais;
- Direito de portabilidade, isto é, de realizar a transferência dos dados a outro agente de tratamento;
- Direito de oposição: o titular poderá se opor ao tratamento de dados pessoais com base legal que não seja do seu consentimento.

Vale destacar que a Lei prevê que os titulares de dados pessoais devem exercer seus direitos perante o controlador de dados pessoais. Quando o controlador recebe um pedido para o exercício de direitos dos titulares de dados pessoais, ele deverá informar, de maneira imediata, aos operadores para que estes possam repetir o mesmo procedimento (isto é, realizar a correção, a eliminação, a anonimização ou o bloqueio dos dados). É de responsabilidade do controlador garantir que os operadores cumprirão tais determinações.



7. O que é agente de pequeno porte? E tratamento de alto risco?

A Resolução da ANPD nº 2/2022 cumpre previsão da LGPD de criar tratamento jurídico diferenciado para que agentes de tratamento de pequeno porte – como micro e pequenas empresas, startups e organizações sem fins lucrativos – se adequem à legislação. A ideia é gerar uma série de regras mais simples para essas pessoas jurídicas, davido a sua estrutura reduzida de funcionamento em relação a grandes empresas, desde prazos em dobro para atendimento das requisições de titulares, até registro resumido das atividades de tratamento da organização. São dois requisitos centrais para que um agente seja configurado como de pequeno porte: (i) ter receita bruta inferior a 4.8 milhões de reais ao ano (ou 16 milhões, no caso de startups), considerando, inclusive, o grupo econômico do qual faça parte, e (ii) não realizar tratamento de alto risco.

É considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico previsto na referida resolução.

Dentre os critérios gerais, estão o tratamento de dados pessoais em larga escala e o tratamento de dados pessoais que possam afetar significativamente interesses e direitos fundamentais dos titulares. Já dentre os critérios específicos, estão o uso de tecnologias emergentes ou inovadoras; a vigilância ou controle de zonas acessíveis ao público; as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais; e a utilização de dados pessoais sensíveis ou de dados pessoais de crianças, adolescentes e idosos.

8. O que são incidentes de proteção de dados pessoais?

Os incidentes de proteção de dados pessoais são quaisquer eventos adversos confirmados, relacionados à violação na segurança de dados pessoais, tais como acesso não autorizado, acesso acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Em caso de incidente de segurança relacionado a dados pessoais que possa acarretar risco ou dano aos titulares daqueles dados (como vazamentos), algumas medidas devem ser tomadas pelas entidades. A LGPD afirma que o titular de dados pessoais deverá ser comunicado acerca do incidente em um prazo razoável, com uma notificação detalhada sobre a natureza do incidente, os riscos envolvidos, bem como as medidas adotadas. A própria autoridade também precisará ser informada sobre qualquer incidente.

Assim, em caso de identificação de qualquer incidente de segurança, é relevante entrar em contato com o departamento jurídico da OSC assim que possível para que se possa avaliar a necessidade de notificar os titulares de dados pessoais e a ANPD.

9. Quais procedimentos básicos devo adotar para adaptar uma organização à LGPD?

Este é um tópico que demanda cautela, pois o processo de adaptação de cada organização dependerá de suas particularidades. Ainda que existam procedimentos gerais que podem ser adotados para garantir essa adequação, o processo em concreto sempre vai depender das características particulares da entidade. Em linhas gerais, visar ao estabelecimento de uma consolidada governança de dados é o pilar central para esse caminho de adequação. Nesse sentido, pensar em limitação dos acessos, realizar data mapping, elaborar fluxogramas para a construção de protocolos de tratamento, formular uma política de privacidade, adotar medidas para segurança da informação, são alguns exemplos que podem ser citados.

Além disso, como já mencionado, a LGPD determina a necessidade de se adotar um encarregado (também por vezes chamado de Data Protection Officer – DPO, em referência à nomenclatura europeia) para a organização que

realiza o tratamento de dados. O encarregado pode ser pessoa física ou jurídica e deve ter suas informações de contato de fácil acesso, sendo responsável por promover cultura e capacitação em proteção de dados. Há, no entanto, a possibilidade de flexibilização da exigência de um DPO por meio da norma para agentes de tratamento de pequeno porte, que ainda está em processo de consolidação pela ANPD.

A formalização jurídica das operações que envolvem tratamento de dados, como dito anteriormente, é essencial para delimitar as obrigações e responsabilidades dos agentes de tratamento, além de garantir os direitos resguardados aos destinatários das ações desenvolvidas pelas OSC. Cabe citar, ainda, o Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte, lançado pela ANPD, em outubro de 2021. O guia indica medidas administrativas e técnicas de segurança da informação e é acompanhado por um checklist que serve para facilitar a visualização das sugestões que devem ser adotadas por esses agentes.

Nota-se, assim, que a ANPD vem, a cada dia, voltando mais sua atenção para a delimitação dos procedimentos básicos que as organizações da sociedade civil deverão adotar para estarem adaptadas à Lei.

10. Quais as principais punições que as organizações poderão sofrer por não se adequarem à LGPD?

De forma geral, a LGPD prevê que o tratamento inadequado de dados pessoais poderá acarretar multa de até 2% do faturamento, com limite de até R$ 50 milhões[5], além da possibilidade de bloqueio dos dados utilizados, podendo até inviabilizar alguns modelos de negócios. Além disso, no caso das organizações da sociedade civil, a punição que pode ocorrer é, principalmente, reputacional, pois uma adaptação precária à nova Lei pode acabar ocasionando um afastamento de potenciais financiadores que buscam entidades devidamente regularizadas nessa matéria.

Quanto às hipóteses de responsabilização, a LGPD prevê essa possibilidade nos âmbitos administrativo e cível. No primeiro caso, caberá à ANDP conduzir um processo que assegure o contraditório, a ampla defesa e o direito de recurso nessa averiguação de uma possível violação ao texto legal. Nesse sentido, a responsabilização dependerá de qual posição está sendo ocupada na cadeia de tratamento.

5 Ainda que se saiba que as OSCs não possuem faturamento, em razão de sua natureza jurídica, a Lei não traz uma base de cálculo alternativa para que se estime o valor da multa.

Tanto o controlador quanto os operadores poderão ser responsabilizados por infrações à Lei, podendo a ANPD aplicar uma série de outras sanções administrativas que não somente a multa (advertência com prazo para adoção de medidas corretivas, bloqueio dos dados pessoais a que se refere a infração até a sua regularização, entre outras medidas).

Em relação à responsabilidade na esfera cível, a LGPD dedica-se inteiramente a explicar a forma como aconteceu essa reparação por parte do agente violador. Essa reparação poderá ser solidária, com algumas hipóteses à qual o operador apenas responde solidariamente se tiver descumprido obrigações da Lei ou não tiver seguido as instruções do controlador. Além disso, o operador poderá ser responsabilizado a ressarcir o dano causado pela violação das medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

A responsabilidade na reparação de danos em vazamentos de dados não foi expressamente definida pela LGPD como subjetiva (depende do dolo/culpa do agente) ou objetiva (independe de dolo/culpa) e essa é uma discussão que está cada vez mais manifesta devido à sua relevância. No entanto, recentes julgados do Tribunal de Justiça de São Paulo (como no caso Cyrela e no caso Serasa, em 2021) apontam para a tese de que só haverá reparação de danos quando a entidade não realizar todos os esforços possíveis para evitar o incidente de segurança.

III.O que fazer para que sua organização possa estar adequada à LGPD

Maraísa Rosa Cezarino[6]

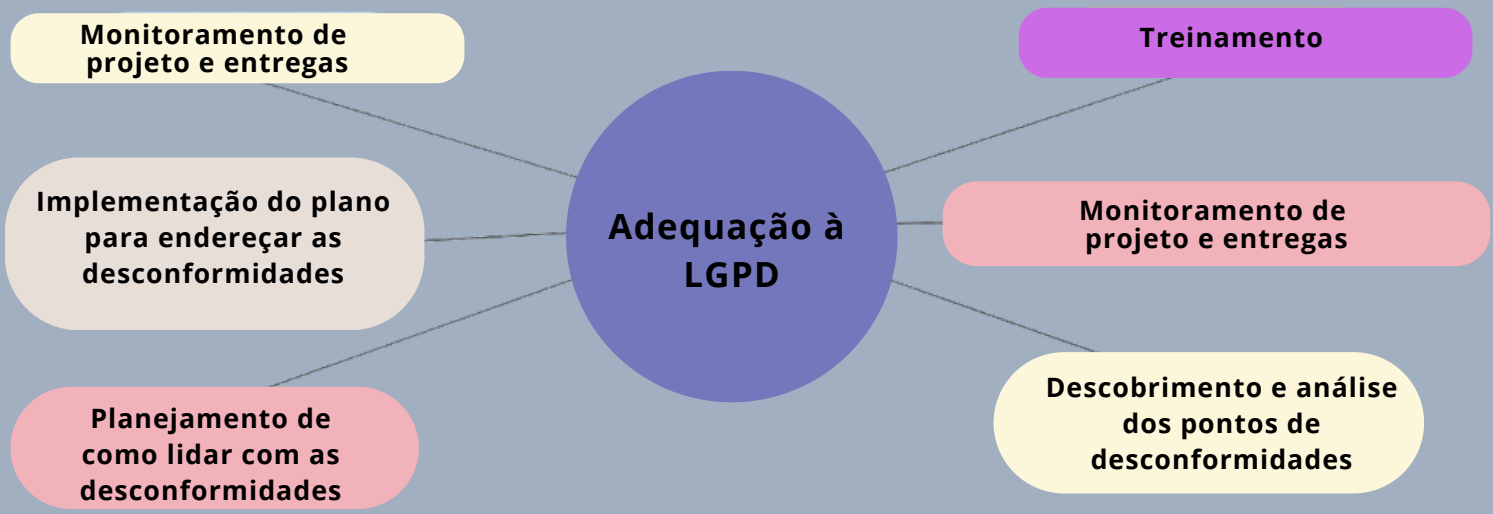
[6] Graduada em Direito pela Universidade de São Paulo e mestranda na mesma instituição. Integrou o Núcleo de Prática Jurídica em Direitos Humanos. Membro do escritório Daniel Advogados. Consultora de organizações da sociedade civil, especialmente quanto à adequação à LGPD.

A LGPD se aplica às Organizações da Sociedade Civil (OSC) de forma que é uma obrigação legal, que pode ser fiscalizada pelas autoridades responsáveis, que as atividades de tratamento de dados pessoais estejam adequadas à Lei. Mas será que esse é o único motivo que deve impulsionar a preocupação com a conformidade das organizações a essa nova Lei?

É importante compreender que, muito além da obrigação legal, adequar as atividades significa garantir a efetividade do direito fundamental à Proteção de Dados Pessoais, previsto na Constituição Federal, desde 2022. Os dados pessoais formam a personalidade digital dos cidadãos, por isso, proteger os dados das pessoas é proteger a sua própria personalidade. A proteção de dados é um ato de cuidado com os/as beneficiários/as e colabores/as das OSCs.

Além disso, não custa lembrar que, outro bom motivo para entrar em conformidade com a Lei é a atração de investimentos externos. Ao redor do mundo, leis parecidas com a LGPD foram aprovadas nos últimos tempos, isso quer dizer que os financiadores passaram a exigir que as organizações receptoras de seus recursos comprovem a sua adequação às leis de proteção de dados dos países onde atuam. Não é incomum ver o envio de grandes questionários de verificação de conformidade para a submissão do envio de verba aos beneficiários de suas ações.

Sugestão de etapas para iniciar e desenvolver um programa de adequação à LGPD:



Vamos lá?

Primeiro passo: Conscientização e definição de objetivos

“Andorinha sozinha não faz verão.”

Nessa primeira etapa do programa, a ideia é ganhar os corações e mentes dos colaboradores para o projeto de adequação. É importante que as pessoas abracem o projeto de adequação com quem está à frente de suas ações!

Não é possível fazer um plano de adequação sem que as pessoas compreendam a importância de estar em conformidade com a Lei. Principalmente, é preciso que a alta direção da organização compreenda a importância da adequação à Lei, pois serão necessárias ações de investimento, de engajamento e de dedicação para atingir a conformidade de uma organização.

Para essa etapa, é necessário pensar em um treinamento sobre os principais pontos da Lei: conceitos, importância, como ela afeta as atividades da organização, as justificativas disponíveis para tratar os dados pessoais etc. É importante adotar um tom que garanta um efeito de acalmar os ânimos em relação à Lei, lembrando que a LGPD não foi feita para impedir os fluxos de dados, mas para proteger as pessoas sobre quem os dados pessoais falam.

Abordagens possíveis para o treinamento	Métodos de aprendizado ativo possíveis
• Roda de conversa	• Formar grupos para mapear as atividades de tratamento de dados em cada área
• Evento com um/a especialista	• Exercícios de simulação de situações que podem demandar aplicação da Lei
• Aula	• Oficina de aviso de privacidade
• Vídeo	• Oficina de mapeamento
• Debate	• Exercícios com alternativas para fixar conceitos

Sugerimos que uma apresentação sobre a Lei Geral de Proteção de Dados seja apoiada por um profissional da área, mas, se isso não for possível, confira os pontos imprescindíveis dentro da apresentação:

Quem a Lei protege (Art. 1)	**Quando a Lei não se aplica (Art. 4)**	**Como a Lei impacta A Organização**
Conceitos importantes para interpretar a Lei (Art. 5)	**Apresentação do cronograma do projeto e dos responsáveis**	**Apresentação de documentos que serão produzidos**

Segundo passo: mapeamento - entendendo quando e como tratamos os dados pessoais

"Conhecimento é poder."

Feita a conscientização, é hora de passar para uma etapa um pouco mais difícil do projeto, o mapeamento de atividades de tratamento. A LGPD, em seu Art. 37, prevê a obrigação de manutenção de registro de operações de tratamento de dados pessoais. Essa obrigação é prevista para o controlador e o operador dos dados pessoais, logo, qualquer agente de tratamento tem a obrigação de mapear os processos que tratam dados pessoais.

O mapeamento dos dados é uma das etapas principais para a manutenção de um programa de governança eficaz, isso por que é ele que permite identificar qual a justificativa (base legal) ideal para cada atividade de tratamento de dados identificada. Com um mapeamento de dados pessoais, é possível identificar qual área é responsável pelo tratamento dos dados pessoais de um titular que, por exemplo, solicite algum de seus direitos previstos no Art. 18 da LGPD.

É importante que, independentemente da forma que o mapeamento seja realizado, o entrevistado e/ou respondente deve ser uma pessoa inteirada do processo e conheça as nuances do tratamento de dados pessoais, pois uma mudança pode impactar diretamente na definição dos agentes de tratamento e/ou definições das bases legais. Na etapa da realização de entrevistas, sugerimos que as seguintes perguntas sejam feitas, sobre **cada atividade de tratamento de dados identificada:**

- Quais são as finalidades para aqueles dados tratados?
- Os dados são estritamente necessários para o tratamento?
- Há tratamento de dados pessoais sensíveis? Se sim, quais?
- Como os dados pessoais entram na organização?
- Por quais tratamentos cada tipo de dados passa, em que área e/ou projeto da organização?
- Há compartilhamento de dados pessoais com terceiros? Quando? Por qual motivo? E com quem?
- Há transferência internacional de dados pessoais?
- Onde as informações pessoais são armazenadas?
- Há descarte dos dados pessoais?

Mais do que cumprir a Lei, o mapeamento é uma oportunidade de obter conhecimento sobre como estão ocorrendo as ações da organização e demonstrar a aplicação da Lei em várias atividades. Sugerimos que a fase de mapeamento percorra as seguintes etapas:

ETAPA	FORMATO SUGERIDO	ENVOLVIDOS
Definições de pontos focais do projeto dentro da organização	Reunião	• Encarregado de proteção de dados • Dirigentes • Pessoas responsáveis pelo projeto de adequação
Definição de atividades a serem mapeadas	Grupos focais	• Pessoas responsáveis pelo projeto de adequação • Gestores das áreas da organização • Pessoas à frente de projetos
Realização de entrevistas	• Reuniões • Formulários colaborativos (Ex: Googleforms)	• Gestores das áreas da organização • Pessoas à frente de projetos grandes
Registro de atividades	• Planillha • Software de Gestão	• Encarregado de proteção de dados • Pessoas responsáveis pelo projeto de adequação

CONTINUIDADE

RECOMENDA-SE QUE O MAPEAMENTO DOS DADOS SEJA ATUALIZADO A CADA NOVO PROCESSO QUE SURJA NA ORGANIZAÇÃO E A REALIZAÇÃO DE UM RE-MAPEAMENTO, PELO MENOS, A CADA UM ANO.

Terceiro Passo: Descobrimento e análise dos pontos de desconformidade

Após a etapa de mapeamento, normalmente, identificamos diversos pontos de desconformidade com a Lei. Esse é mesmo um dos objetivos do mapeamento.

Mas, calma, não precisa ficar nervoso/a! A ideia aqui é traçar os problemas e identificar as oportunidades de melhoria das atividades, de forma a garantir a adequação de cada uma delas.

Analise cada atividade para entender o que pode estar em desconformidade com os princípios e obrigações da Lei: a forma de coleta de dados? Qual a quantidade de dados coletados? A falta de transparência no tratamento dos dados pessoais?

Identifique o que está incorreto e o que pode melhorar.

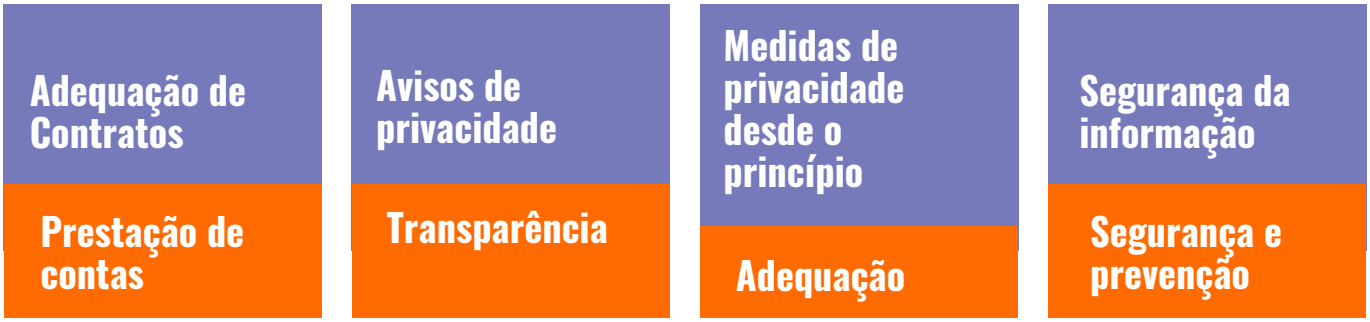
Quarto Passo: Planejamento de como lidar com as desconformidades mapeadas

Com os problemas e pontos de atenção registrados, faça um plano para lidar com as desconformidades identificadas. Para isso, é preciso traçar prioridades: o que gera mais risco para a organização? Isso é o que deve ser tratado primeiro.

O que gera um risco médio e baixo? Isso será tratado depois.
Organize as medidas e documentos que serão implementados na construção da estrutura de conformidade na qual a organização está trabalhando. Além disso, identifique a base legal correta para cada atividade.

Quinto passo: Implementação das medidas de adequação elencadas no plano para endereçar as desconformidades

- Passada a fase de mapeamento dos dados e identificadas as lacunas, e, após a elaboração de um plano de ação, inicia-se a fase de implementação das medidas de adequação. Dentro dessa etapa, elencamos as principais medidas normalmente utilizadas para entrar em conformidade com a LGPD:



A Adequação de Contratos

Revisar contratos é fundamental para estabelecer os termos e condições das relações com parceiros, estabelecer requisitos e definir as responsabilidades dos agentes de tratamento envolvidos. Um bom contrato de tratamento de dados pessoais deve abordar questões controvertidas da Lei e aquelas ainda não regulamentadas pela ANPD, como, por exemplo, a transferência internacional de dados pessoais. Alguns dos tópicos que devem ser considerados em um contrato de tratamento de dados pessoais incluem:

DEFINIÇÃO DOS AGENTES DE TRATAMENTO

A definição dos agentes de tratamento é essencial para a definição e limitação de responsabilidade de atuação das partes. Conforme disposto na LGPD, em seu Art. 39, o operador realiza o tratamento dos dados pessoais conforme as instruções fornecidas pelo controlador, logo, cabe ao controlador as principais responsabilidades acerca do tratamento dos dados pessoais.

COOPERAÇÃO ENTRE OS AGENTES DE TRATAMENTO PARA O CUMPRIMENTO DE:

Solicitação de autoridades judiciais e/ou administrativas; atendimento aos direitos dos titulares; avaliação de incidentes; avaliação de necessidade de notificar à ANPD.

DELIMITAÇÃO DO TRATAMENTO DOS DADOS PESSOAIS ABORDANDO OS SEGUINTES PONTOS:

Dados pessoais a serem tratados; transferência internacional dos dados pessoais; limitação temporal do armazenamento dos dados pessoais; e base legal definida para o tratamento dos dados.

DEVER DE INDENIZAR E DIREITO DE REGRESSO

Em caso de descumprimento do estabelecido no termo ou no contrato, a Parte que descumpriu deverá indenizar a outra Parte. Caso o descumprimento resulte em: ações judiciais; ações administrativas; ações movidas por titulares; multas imputadas por autoridades, a parte que sofreu os danos mencionados terá o direito de reivindicar os danos suportados.

NOTIFICAÇÃO EM CASO DE INCIDENTE DE SEGURANÇA

A LGPD estabelece que o controlador deve notificar a APND em caso de incidente com dados pessoais. Até o momento, a ANPD recomenda que a notificação seja realizada em até dois dias.

Avisos de privacidade (Política de Privacidade)

O aviso de privacidade é um documento que visa atender ao princípio da transparência (Art. 6, VI da LGPD) bem como os requisitos previstos no Art. 9 da LGPD para atender ao princípio do livre acesso, através dele o controlador deve fornecer as seguintes informações ao titular, veja abaixo o que não pode faltar nesse aviso:

- Para que queremos os dados pessoais?
- Como e até quando tratamos os dados?
- Com quem a organização pode compartilhar os dados nessas atividades?
- Quem é o controlador dos dados?
- Como entro em contato se eu quiser exercer direitos?
- Quais são os direitos dos titulares?

É recomendado que o aviso seja exposto onde o titular de dados pessoais possa visualizar e entender de que forma ocorre o tratamento dos seus dados pessoais, como, por exemplo, um aviso de privacidade disposto em um site, aplicativo ou formulário (físico e/ou digital). Ainda, o aviso deve ser elaborado em uma linguagem que seja compreensível para todos os titulares.

Privacidade desde a concepção (Privacy by design - PbD)

A adoção da privacidade desde a concepção do projeto e/ou novo processo é importante não apenas para o titular do dado pessoal, mas também para a organização, pois a aplicação correta da abordagem pode evitar diversas ações judiciais, administrativas ou multas, porque o cenário foi previamente avaliado pela organização. O conceito de privacidade desde a concepção possui sete princípios norteadores, são eles:

Princípio	Na prática
1.Abordagem proativa e não reativa;	Avisar que os dados estão sendo coletados e compartilhados sem que ninguém pergunte a respeito.
2.Sistemas, serviços e produtos devem proteger os dados pessoais;	Manter os cookies e outros mecanismos como captação de geolocalização desativados e permitir que o usuário entenda e escolha fornecer os seus dados.
3.O design deve ser incorporado às medidas adotadas para a proteção de dados pessoais;	
4.Tratar apenas os dados pessoais necessários;	Fazer formulários e aplicativos com a captação do menor número de dados pessoais possível.
5.Adotar medidas de segurança que sejam aplicáveis do início ao fim do tratamento;	Criptografia para os dados em repouso e dados em trânsito; Autenticação de múltiplo fator.
6.Adotar visibilidade e transparência;	Elaborar e disponibilizar aviso de privacidade sobre o tratamento de dados pessoais.
7.Respeitar a privacidade do titular.	Analisar todo o fluxo de tratamento de dados partindo do pressuposto de que a privacidade e a proteção dos dados pessoais do titular são um direito fundamental.

Para auxiliar a aplicação da privacidade desde a concepção, a agência de *protección de datos* publicou um guia orientativo de boas práticas. O guia pode ser acessado neste QRCODE ou no link.

Políticas de Segurança da Informação

Uma política de segurança de informação é um conjunto de regras e diretrizes que visam proteger os dados e os sistemas de informação de uma organização. Ela estabelece as responsabilidades e os procedimentos que devem ser seguidos para garantir a confidencialidade, integridade e disponibilidade da informação. Além disso, uma política de segurança de informação também pode incluir medidas para proteger a privacidade dos usuários e evitar violações de dados.

A disciplina da Segurança da Informação é organizada a partir dos seguintes princípios:

Confidencialidade	Garantir que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados.
Disponibilidade	Garantir que as informações estejam sempre disponíveis para uso pelas pessoas autorizadas.
Integridade	Proteger a exatidão da informação.
Autenticidade	Garantir que as informações só possam ser acessadas por pessoas autorizadas e confirmar a identidade dessas pessoas.
Não repúdio	Provar a ocorrência de um suposto evento ou ação e suas entidades de origem.
Responsabilidade	Garantir que as pessoas responsáveis pelo gerenciamento da informação sejam identificadas e tenham a responsabilidade.

No ano de 2021, a Autoridade Nacional de Proteção de Dados lançou um guia orientativo de segurança da informação para agentes de tratamento de pequeno porte, que pode ser lido acessando este link ou QRCODE:

Uma política de segurança da informação deve tratar sobre medidas técnicas e organizacionais que ajudem a garantir que as informações estejam sempre disponíveis, protegidas contra acessos indevidos e alterações não autorizadas. Para ilustrar os dois tipos de medidas, elaboramos essa tabela exemplificativa:

Medidas Técnicas	1. Criptografia para os dados em repouso e em trânsito; 2. Análise de Vulnerabilidade; 3. Teste de Invasão; 4. Antivírus; 5. Modem que possua criptografia; 6. Manutenção dos logs de acesso; 7. Mecanismos para evitar ataques brute force; 8. Captcha para logins e/ou envio de mensagens; 9. Autenticação de Múltiplo Fator; 10. Bloqueio automático de dispositivos; 11. VPN; 12. Armários com chave; 13. Backups realizados em outros locais fora do servidor; 14. Controle de acesso; 15.Extintores de incêndio.
Medidas Organizacionais	1. Política de senha forte; 2. Política de mesa limpa; 3. Política de Resposta a Incidente; 4. Treinamentos; 5. Conscientização por pílulas.

Além disso, é importante entender quais são os tipos de ameaça mais comuns no espaço da internet, pois a Política deve conter indicativos de como prevenir que elas ocorram:

Fator humano	• falta de treinamento adequado em segurança da informação; • negligência de indivíduos responsáveis pelos sistemas da organização ou que têm acesso a eles.
Phishing	• envio de comunicações falsas que parecem vir de uma fonte confiável; • geralmente entregues através de email, mas também através de SMS ou outros meios; • o objetivo é roubar informações confidenciais, como números de cartão de crédito e credenciais de login, ou instalar malware no dispositivo da vítima.

Trojan

- é um tipo de malware que se esconde em um aplicativo ou arquivo legítimo e é instalado no computador da vítima sem o seu conhecimento ou consentimento;
- instalado, o trojan pode controlar o computador da vítima, roubar informações confidenciais ou realizar outras ações maliciosas sem que a vítima perceba.

Spyware

- tipo de software malicioso que se esconde em um computador sem o conhecimento ou consentimento do usuário e coleta informações sobre ele sem que ele saiba;
- usado para rastrear o histórico de navegação do usuário, coletar suas credenciais de login e senha, ou até mesmo vigiar o usuário através da webcam;
- geralmente distribuído por downloads gratuitos ou de cliques em links maliciosos.

Ransomware

- realiza o "sequestro" dos dados, os dados sequestrados são criptografados e exige que o usuário pague um resgate para reaver aquelas informações;
- O pagamento do resgate não garante que as informações sejam reavidas pelo usuário.

Política de Resposta a Incidente de Segurança da Informação

Primeiro de tudo, o que é um incidente? Um incidente de segurança de informação é qualquer evento ou atividade que possa ameaçar a qualquer um dos princípios de segurança da informação de uma organização. Para cada princípio podemos pensar em exemplos de incidentes que vão muito além dos vazamentos de dados:

Confidencialidade	Disponibilidade	Integridade
Vazamento de Dados; Documentos contendo informações pessoais de fácil acesso para terceiros não autorizados.	Ransomware; Destruição de informações; Ataque de negação de serviço (DDoS).	Alterações indevidas nas informações; Injeção de código malicioso.

As ameaças apresentadas impõem a necessidade de ter um plano para lidar com incidentes de segurança que afetem os dados pessoais da organização. Ter um plano que permite o gerenciamento de incidentes de segurança de informação de forma adequada e eficaz, minimizando o impacto na organização. Para que um plano seja eficiente, ele deve passar pelos seguintes pontos:

Definição de incidente

Uma descrição objetiva dos tipos de eventos que serão considerados incidentes e precisam ser reportados.

Processo de reporte

Como os incidentes devem ser reportados e para quem - titulares de dados e autoridades.

Equipe de resposta

Identificação da equipe responsável por gerenciar e investigar os incidentes.

Protocolo de resposta

Etapas a serem seguidas para gerenciar e investigar os incidentes, incluindo a apuração do risco envolvido no incidente, a coleta de evidências e a notificação de autoridades e titulares de dados relevantes.

Treinamento

Plano de treinamento para garantir que todos os envolvidos estejam cientes de suas responsabilidades e saibam como lidar com incidentes de segurança da informação.

Acompanhamento/ registro

Processo para acompanhar o progresso da resposta aos incidentes e registrar o que aconteceu e como lidamos com a situação.

É importante ter em mente que só é necessário notificar a ANPD e os titulares de dados pessoais quando a organização tiver certeza de que o incidente identificado pode ter ocasionado risco ou dano relevante aos titulares dos dados. Portanto, não é qualquer incidente que deve ser notificado. Para elaborar melhor o assunto, recomendamos assistir à seguinte aula: https://www.youtube.com/watch?v=SKVqq9Cg3Io.

A ANPD disponibilizou o formulário de comunicação de incidente de segurança da informação que pode ser baixado direto da internet. O encarregado de proteção de dados ou um representante legal do controlador deve preencher o formulário e enviá-lo eletronicamente através do sistema Peticionamento Eletrônico do SUPER.BR (Sistema Único de Processo Eletrônico em Rede). Durante o envio, é preciso selecionar o tipo de processo "ANPD - Comunicados de Incidentes à Autoridade Nacional de Proteção de Dados" e anexar o formulário preenchido, preferencialmente em PDF, com qualquer documento complementar, como a atribuição do encarregado de proteção de dados, procuração ou contrato social.

Durante o projeto de adequação, a ideia é criar uma estrutura de proteção e governança para os dados pessoais dentro da organização. Uma vez que isso é feito, fica muito mais fácil e orgânico tratar desse tema e responder eventuais questionamentos de financiadores, autoridades e titulares sobre ele.

Acontece que, como qualquer estrutura, aquela criada durante o projeto precisa de manutenção! Nesse sentido, não se pode deixar que o tema da proteção de dados pessoais caia no esquecimento e só ressurja durante uma crise, por isso sugerimos algumas recomendações para garantir a atualidade das medidas criadas e implementadas durante o projeto de adequação:

Como entregas principais do projeto é possível listar as seguintes:

- Registro de atividades de tratamento de dados pessoais (Anexo I)
- Política de Privacidade (Anexo II)
- Plano de resposta a incidentes de segurança (Anexo III)
- Política de Segurança da Informação
- Cláusulas contratuais de proteção de dados pessoais (Anexo V)
- Política interna sobre a estrutura de proteção de dados
- Política de retenção de dados pessoais
- Modelo de teste de legítimo interesse (Anexo IV)

IV. Definição do/a encarregado/a pela proteção de dados da OSC e elaboração de política de governança de privacidade

Manoel Nascimento [7]

[7] Manoel Nascimento é advogado e consultor em proteção de dados.

1. Encarregado pela proteção de dados: definição, atribuições e perfil

1.1. O que é o "encarregado pela proteção de dados"?

Por influência do inglês de negócios, é comum chamar este cargo de *data protection officer*, ou pela sigla DPO. Seguiremos a nomenclatura estabelecida pela legislação brasileira: encarregado pela proteção de dados. É a 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) (LGPD, art. 5º, VIII). A identidade e as informações de contato do encarregado (e-mail ou formulário de contato) deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

1.2. Atribuições

São atividades de um encarregado (LGPD, artigo 41, parágrafo 2º, incisos I a IV):
•Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

•Receber comunicações da autoridade nacional e adotar providências;

•Orientar os funcionários e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

•Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

1.3. Quem precisa indicar um encarregado?

A LGPD obrigou todos os controladores a indicar um encarregado; assim, até recentemente, era necessário assumir como regra que toda OSC deveria indicar uma pessoa para assumir esse papel. Mais à frente, será tratado, como exceção, o caso das organizações e empresas de pequeno porte, para quem esta regra foi flexibilizada (sob certas condições) pela Resolução CD/ANPD nº 2.

1.4. Perfil profissional do encarregado

A LGPD não indica um perfil obrigatório para o exercício da função. Por isso, não há previsão de formação específica para que alguém atue como encarregado, tampouco se impõe a exigência de diploma universitário ou técnico. Apesar disso, verifica-se uma tendência à contratação de profissionais com formação técnica ou universitária nas áreas de Direito,

Administração, Comunicação Social, Relações Públicas, Jornalismo, Gestão de Mídias Sociais, Engenharia Elétrica, Engenharia de Software, Engenharia da Computação, Ciência da Computação, Sistemas de Informação, Análise e Desenvolvimento de Sistemas, Gestão em Tecnologia da Informação ou qualquer outra carreira na área de tecnologia da informação.

Tem sido comum, também, a contratação de profissionais com pós-graduação em Direito Digital ou áreas correlatas.

Independentemente da formação, espera-se de um encarregado domínio nas seguintes áreas:

•Segurança da informação, de preferência com certificações de conhecimento das normas ISO 27001 e ISO 27002;

•Legislação brasileira e internacional sobre proteção de dados, como a LGPD, o Regulamento Geral de Proteção de Dados (RGPD), da União Europeia, e a Lei de Proteção de Consumidores da Califórnia (CCPA);

•Gestão de tecnologia da informação, de preferência com certificações de conhecimento.

As certificações não são requisito obrigatório, mas provam conhecimento em qualquer das áreas citadas; têm sido bem reputadas no ramo certificações emitidas pela International Association of Privacy Professionals (IAPP), pela Data Privacy Brasil e pela EXIN. Outro excelente indicador é a participação em associações profissionais da área da segurança da informação e da proteção de dados; além da IAPP em escala internacional, no Brasil é bem reputada a Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD).

Espera-se de um encarregado, no mínimo, as seguintes competências:

•Conhecimento jurídico e regulatório: necessário conhecer a LGPD e os regulamentos emitidos pela ANPD, e o básico da legislação internacional (Regulamento Geral de Proteção de Dados (RGPD), da União Europeia, e a Lei de Proteção de Consumidores da Califórnia (CCPA) etc.).

•Tecnologia da informação: deve ter algum conhecimento em TI (programação, sistemas, infraestrutura, redes etc.) para compreender as atividades de tratamento de dados transcorridas sob sua responsabilidade.

•Gestão de riscos: como o encarregado precisa levar em consideração os riscos envolvidos nas operações de tratamento, e também orientar e gerar evidências sobre as medidas de conformidade com o marco regulatório do

setor, deve conhecer o suficiente de gestão de riscos para identificar potenciais riscos, além de entender como certas ferramentas podem auxiliar em medidas de privacidade e segurança por padrão.

•Liderança: o encarregado é assessor direto do nível mais alto de gestão da organização, a quem se reporta diretamente e sem intermediários, e que deve lhe assegurar a autonomia necessária ao exercício de suas funções.

•Proatividade: o encarregado deve tomar a frente das atividades de proteção de dados que ficarem sob sua responsabilidade, sem esperar pela iniciativa de quem quer que seja.

•Senioridade: as responsabilidades envolvidas no cargo exigem que o encarregado tenha a senioridade e a maturidade necessárias para lidar com decisões estratégicas, com pressão para a entrega de resultados, e que tenha capacidade para propor ou desenvolver soluções inovadoras para a melhoria do desempenho na área da privacidade.

•Auditoria: o encarregado atua como fiscal interno da conformidade de uma organização à LGPD e outras normas de proteção de dados; por isso, deve ser proativo e saber como identificar e localizar as informações necessárias para executar seu trabalho.

•Relações públicas: como o encarregado atuará como canal de comunicação com os titulares e com a ANPD, deve ter habilidade para se posicionar adequadamente em nome da organização perante terceiros, desenvolvendo narrativas condizentes com as evidências pertinentes a cada caso, evitando ao máximo jargões técnicos, jurídicos ou de TI.

•Capacidade educativa e pedagógica: cabe ao encarregado coordenar o treinamento da equipe da organização nos temas da segurança da informação e da proteção de dados, e servir como elemento de apoio da equipe em caso de dúvidas quanto a certos aspectos das operações de tratamento de dados.

•Outras habilidades pessoais e interpessoais: pela natureza do cargo, é de se esperar que um encarregado tenha boa oratória; que conheça inglês o suficiente para comunicar-se com outros encarregados de organizações sediadas em outros países; que tenha boa capacidade de argumentação e conhecimento em técnicas de negociação para lidar com eventuais reclamações e investigações nos casos de tratamento irregular de dados; e, principalmente, que tenha experiência prévia no ramo em que a OSC está envolvida, para avaliar corretamente os riscos da atividade e propor as soluções mais adequadas a cada caso.

O conhecimento prático e a experiência comprovada poderão ser requisitos futuros ao avaliar a contratação de um encarregado. Não obstante, o cargo é de criação recente (2018), e sua indicação como requisito obrigatório para o tratamento de dados é ainda mais recente (2020). Não se pode esperar que em tão pouco tempo haja profissionais com longa experiência na função. No momento, é recomendável dar menos peso à experiência, exigindo-se como contrapartida maior ênfase nas demais competências.

A LGPD nem proíbe, nem determina se o encarregado deve ser pessoa física ou jurídica, tampouco diz se deve ser funcionário da organização ou agente externo. Cabem todos esses perfis, desde que o encarregado seja constituído por um ato formal, como um ato administrativo de nomeação (para encarregados funcionários da organização) ou um contrato de prestação de serviços (para encarregados externos).

A LGPD nem proíbe, nem obriga que um mesmo consultor, independente ou pessoa jurídica, atue como encarregado em nome de diferentes organizações. É importante avaliar sua capacidade de realizar com eficácia o trabalho contratado antes de finalizar a contratação, porque a responsabilidade pelas atividades de tratamento de dados pessoais continua sendo do controlador ou do operador de dados (LGPD, art. 42) e uma falha do encarregado pode envolver a OSC em irregularidades no tratamento de dados pessoais.

A LGPD nem proíbe, nem exige que o encarregado seja apoiado por uma equipe de proteção de dados. Considerando as boas práticas e a grande carga de responsabilidade, é importante que tenha recursos adequados para realizar suas atividades, o que pode incluir recursos humanos, tempo (prazos apropriados), finanças e infraestrutura.

2. Programa de governança em privacidade (conteúdo, publicização e implementação)

2.1. Contexto e definição legal

Para estar em conformidade com o marco regulatório da proteção de dados, não é suficiente colocar aviso de privacidade e cookies em websites; uma OSC deve levar a proteção de dados em conta também em suas atividades administrativas (folha contábil, contratação de planos de saúde coletivos etc.), em seus contratos e em vários outros âmbitos em que são realizadas operações de tratamento de dados. Embora seja importante o aviso de privacidade e cookies, ele não orienta nenhuma dessas outras atividades, porque não implementa a privacidade como prática transversal às atividades da OSC.

Ao documento mais amplo, que sistematiza as boas práticas em privacidade da OSC em todas as suas operações de tratamento de dados, dá-se o nome de programa de governança em privacidade. A LGPD não o tornou obrigatório para quem realiza tratamento de dados, mas estabelece vantagens para aqueles que o fizerem (a exemplo da atenuação de sanções em caso de tratamento irregular ou incidentes de segurança). Além disso, ele prova que o tratamento de dados na OSC atende aos princípios da transparência, segurança e prevenção (art. 6º, VI, VII e VIII da LGPD).

2.2. Conteúdo mínimo de um programa de governança em privacidade

O programa de governança em privacidade é um dos produtos finais de um processo de diagnóstico das operações de tratamento de dados realizadas pela OSC, coordenado por profissional especializado (seja um encarregado pela proteção de dados já contratado pela OSC, seja uma consultoria externa).

O conteúdo dos programas de governança em privacidade é determinado pelo resultado desse diagnóstico, e pelos parâmetros estabelecidos pelo artigo 50 da LGPD. Por ele, os agentes de tratamento de dados poderão, individualmente ou por meio de associações, formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos (incluindo reclamações e petições de titulares), as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Ao estabelecer tais regras, as OSCs que realizam operações de tratamento de dados deverão levar em conta a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes dessas mesmas operações.

Para assegurar respeito aos princípios da segurança e da prevenção (art. 6º, VII e VIII da LGPD) e estar em conformidade com o marco regulatório brasileiro de proteção de dados pessoais, o programa de governança em privacidade deve observar, no mínimo, os seguintes requisitos (LGPD, art. 50, §2º, I, a até h):

a) Demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) Ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) Ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) Estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) Ter como objetivo estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) Estar integrado a sua estrutura geral de governança, além de estabelecer e aplicar mecanismos de supervisão internos e externos;

g) Contar com planos de resposta a incidentes e remediação; e

h) Ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Além disso, em respeito aos mesmos princípios, a organização deverá demonstrar a efetividade de seu programa de governança em privacidade quando apropriado. Essa obrigação tem ainda mais peso quando solicitada pela ANPD ou por qualquer outra entidade independente responsável por promover o cumprimento de boas práticas ou códigos de conduta.

O programa deve demonstrar conhecimento do fluxo de dados sob a responsabilidade da OSC, evidenciando em quais momentos ocorre o emprego de dados pessoais; quais são os dados tratados; como e por quem esses dados foram coletados; como a utilização desses dados se relaciona com a atividade desenvolvida pela organização; como se dá o processamento dos dados, uma vez que ingressam na organização; e como saem do controle da organização (descarte, transferência etc.).

O programa deve evidenciar que existe na OSC um nível de organização compatível com o risco da atividade, assegurando que sua estrutura é capaz de cumprir com as determinações legais e de proteger todo o conjunto de dados pessoais sob seu controle, independentemente do modo como se realizou sua coleta.

No programa devem estar indicados os responsáveis por sua implementação e o monitoramento, detalhando-se a coordenação dos diversos membros dentro da organização, podendo, inclusive, designar indivíduos em cada área da entidade para serem responsáveis pelo programa e para apoiarem sua implementação setorial.

O programa também deve conter um processo de conformidade com a LGPD na contratação de parceiros; um plano de resposta a incidentes de segurança da informação; instrumentos de detecção e remediação das condutas incompatíveis com as boas práticas estabelecidas no programa, indicando também mecanismos de investigação dos responsáveis por violações à política e seu adequado sancionamento.

Na redação dos documentos do programa de governança em privacidade, deve-se respeitar o princípio da transparência (LGPD, art. 6º, VI), adotando linguagem simples, capaz de transmitir informações precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. Portanto, o uso de jargões da Informática ou do Direito é desaconselhado, recomendando-se redação focada na compreensão por usuários leigos; do contrário, viola-se o direito dos titulares ao acesso facilitado às informações sobre o tratamento de seus dados (LGPD, art. 9º).

2.3. Quais documentos devem compor um programa de governança em privacidade?

Para ser efetivo e eficaz, o programa deve estabelecer códigos de ética e conduta para as atividades de tratamento de dados realizadas sob responsabilidade da OSC, com o seguinte conteúdo mínimo:

•Estabelecer as condições de organização, o regime de funcionamento, os procedimentos (inclusive as reclamações e as petições de titulares), as normas de segurança, os padrões técnicos, as obrigações específicas para todos os envolvidos, as ações educativas a serem empreendidas e os mecanismos de supervisão e mitigação de riscos;

•Explicitar quais dados podem ser tratados, em quais hipóteses, e para quais finalidades;

•Prever minuciosamente os comportamentos a serem adotados para cada hipótese de tratamento;

•Estabelecer instrumentos de alerta para as situações mais sensíveis de tratamento, que envolvam maior risco para os titulares dos dados;

•Orientar os funcionários a revelarem a realização de tratamento de dados, assim como realizarem-na somente quando necessário;

•Recomendar o período de armazenamento autorizado dos dados e a sua revisão periódica, bem como determinar a modalidade de guarda de dados;

•Estabelecer quais funcionários podem acessar que espécie de informações (política de acesso controlado);

•Indicar a obrigação de manter registro de todo tratamento realizado;

•Destacar as hipóteses de compartilhamento de dados e os requisitos de tal compartilhamento, em especial quando se tratar de transferência internacional de dados pessoais;

•Prever os requisitos necessários para a contratação de parceiros em atividades que envolvam tratamento de dados (exigência de certificações ou de evidência de adoção de política de governança como requisito para a celebração de acordo, a adoção de cláusulas-padrão contratuais etc.);

•Estabelecer relação de confiança com o titular, por meio de atuação transparente e de instrumentos de sua participação.

Além desses documentos de mais amplo alcance, o programa deve estabelecer:

•Política de proteção de dados para os trabalhadores e prestadores de serviço da OSC, contendo termos de consentimento para o tratamento de dados a serem assinados pelos trabalhadores e prestadores de serviço como aditivos a seus contratos. Há um modelo dessa política nos anexos.

•Para as OSCs que têm website, um aviso de privacidade e cookies, e uma política de privacidade específica para os visitantes do website e usuários dos demais elementos da presença digital da organização (boletim de e-mail, notificações, e-commerce etc.), que envolva termos de consentimento específicos para cada atividade. Um modelo de política de privacidade e cookies é fornecido em anexo a este material didático, assim como um link para o manual orientativo da ANPD. Pode-se também recorrer a serviços que automatizam a criação do aviso e da política, como AdOpt (https://goadopt.io/), Dogma Data Privacy (https://www.dogma.legal/) e Securiti Privacy Center (https://securiti.ai/privacy-center/).

2.4. Quais documentos do programa de governança em privacidade devem ser disponibilizados ao público?

Cada documento deve estar disponível somente para aqueles a quem seu conteúdo se direciona.

Os códigos de ética e conduta, assim como os procedimentos e controles internos, são documentos de circulação interna à OSC. Devem ser apresentados e discutidos com todos os trabalhadores e prestadores de serviço, além de serem base para atividades de treinamento e reciclagem de conhecimento da equipe. A OSC poderá colocá-los em seu website como parte de programas de transparência institucional, desde que sua divulgação não prejudique o sigilo profissional, a ética e o andamento normal de certas operações, e que não represente risco para a OSC ou para terceiros.

A política de proteção de dados para os trabalhadores e prestadores de serviço é um documento de circulação interna à OSC, que deve ficar sob a guarda do setor administrativo da OSC e ser disponibilizada somente àqueles a quem se destina.

Um aviso de privacidade e cookies deve estar disponível no website da organização a cada novo acesso. A política de privacidade do website deve estar acessível aos visitantes por meio de um link que deve poder ser visto e clicado a partir de qualquer página do website. Os dois documentos devem ser apresentados no website de forma clara, acessível e ostensiva, sem necessidade de clicar em várias páginas sucessivas até acessar seu conteúdo.
A divulgação no website da organização de outros documentos específicos de seu programa de proteção de dados deve ser avaliada caso a caso, levando sempre em consideração a necessidade dessa publicação e também o sigilo profissional, a ética, o andamento normal de certas operações e uma avaliação do risco da publicização para a OSC ou para terceiros.

2.5. Programas coletivos: uma alternativa autorregulada

O artigo 50 da LGPD orienta que regras de boas práticas de governança também podem ser formuladas por meio de associações, que devem ser entendidas como qualquer entidade representativa de organizações (de um ramo profissional, cidade, estado, bioma, região, temática afin etc.). No campo sindical, por exemplo, seriam as federações, confederações e centrais sindicais. No campo mais amplo da sociedade civil, seriam associações como a ABONG ou a CNBB.

Como funcionariam esses "programas coletivos" de governança em privacidade? Com regras gerais de boas práticas de governança em privacidade. A associação representativa não tem condições de diagnosticar as operações de tratamento de dados realizadas por cada filiada, nem de produzir um programa de governança em privacidade específico para cada uma delas. Nada impede, entretanto, que promova diálogos entre suas filiadas para pactuar recomendações gerais e orientações que sirvam de parâmetro para a estruturação de programas de governança em privacidade e orientem a construção das políticas simplificadas de segurança da informação por suas associadas de pequeno porte.

3. Monitoramento da política de proteção de dados (importância, como fazer)

Para assegurar a conformidade à LGPD e o aprofundamento de uma cultura de privacidade digital e proteção de dados na OSC, o programa de governança em privacidade de dados deve ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas (LGPD, art. 50, §2º, I, h). Desse modo, o programa deve prever as formas, métodos e ciclos de seu próprio monitoramento.

3.1. Importância

Toda OSC que realiza operações de tratamento de dados deve produzir evidências de que estão em conformidade com a LGPD, e de que os direitos dos titulares são efetivamente respeitados nas operações de tratamento de dados graças ao desenvolvimento e manutenção de uma cultura organizacional de proteção de dados capaz de assegurá-los. O monitoramento registra, guarda e sistematiza essas evidências.

O monitoramento do programa de governança em privacidade envolve o controle, o gerenciamento e a comunicação dos riscos associados com as práticas de gerenciamento da privacidade na OSC. Deve garantir que a forma como a OSC age é a forma como ela diz que age, sem contradição entre documentos de política e a prática de sua implementação e execução. É um processo contínuo, que assegura conformidade, conscientização elevada, transparência e credibilidade, além de auxiliar na identificação de lacunas no programa e prover mecanismos para sua otimização e escala.

3.2. Como fazer

O escopo do monitoramento é a gestão da proteção de dados pessoais e privacidade, e a conformidade do processo de tratamento de dados e de todos os processos e atividades onde exista a manipulação de dados pessoais, sejam eles digitais, eletrônicos ou manuais. Durante o diagnóstico das operações de tratamento de dados na OSC, devem-se identificar os sistemas que não podem ser monitorados, ou que não podem proteger dados pessoais. Eles devem ser alterados, substituídos ou mesmo descontinuados.

3.2.1. Estabelecimento de métricas

Ainda durante o diagnóstico das operações de tratamento de dados, é preciso estabelecer métricas (indicadores, meios de verificação etc.) capazes de comprovar a implementação e o adequado funcionamento das medidas de proteção descritas no programa de governança de privacidade. Métrica é a unidade de medida, a mais objetiva possível, que agregue valor e reflita com precisão o estado dos objetivos e metas da OSC em relação à privacidade.

A identificação das métricas pode ser tarefa complexa, pois deve levar em consideração sua sustentação no tempo e sua escalabilidade por toda a extensão da OSC. Além disso, as métricas devem ser calibradas ao público a que se destinam, com base em seu nível de interesse, influência e responsabilidade com a privacidade. Recomenda-se a adoção de métricas que permitam aumentar o entendimento das proteções necessárias à privacidade, reforçando essa compreensão dentro da OSC. É preciso cuidado, entretanto, para não estabelecer uma quantidade excessiva de métricas; às vezes, a mesma métrica pode ser adaptada de formas diferentes para públicos diferentes da OSC, ou para setores diferentes da OSC, desde que as adaptações não gerem resultados díspares. As métricas devem ser atualizadas de acordo com as mudanças dos objetivos da OSC.

Um exemplo de métrica: estabelecer avisos de privacidade em todos os canais de coleta de dados pessoais. Para atingi-la, a OSC precisaria, por exemplo, implementar o aviso de privacidade em seu website; rever a coleta de consentimento dos destinatários de seu boletim eletrônico enviado por e-mail; colocar um aviso no cabeçalho das listas de presença indicando a finalidade dos dados coletados; entre outras medidas. Ao adotar a métrica, e ao produzir evidência de que ela está sendo cumprida, reforça-se o entendimento de que o aviso de privacidade é um elemento necessário ao tratamento legítimo de dados.

3.2.2. Desenho institucional

O programa de governança em privacidade deverá conter uma sistematização das métricas, e também a indicação de uma pessoa responsável pelo seu monitoramento, que pode ser o encarregado pela proteção de dados ou outra pessoa. Está sob sua responsabilidade monitorar a performance dos processos; conhecer a criticidade de cada métrica, e como isso se adequa aos objetivos da OSC; manter a documentação relacionada ao monitoramento atualizada; revisar regularmente as métricas, para saber se ainda é efetiva e se continua agregando valor, assegurando assim a incorporação e manutenção de melhorias ao monitoramento.

Uma vez coletadas as métricas, elas devem ser analisadas, de preferência, por meios estatísticos. O processo será muito beneficiado se a OSC contar com mecanismos de autoavaliação (questionários, formulários etc.), métodos estruturados ou ferramentas automatizadas como AdOpt (https://goadopt.io/), Dogma Data Privacy (https://www.dogma.legal/), Securiti Privacy Center (https://securiti.ai/privacy-center/) ou 36Zero (https://www.36zero.com.br/).

O monitoramento das operações de tratamento de dados deve ser incluído nos métodos e ciclos de gestão da organização (PDCA, ZOPP, PES, marco lógico, planejamento estratégico etc.) como dimensão independente.

3.2.3. Auditoria externa periódica

Além das atividades internas de monitoramento, é boa prática a contratação de auditorias externas periódicas para o programa de governança em privacidade da OSC. Na sua coordenação, deve-se dar preferência às pessoas e áreas da OSC envolvidas com auditorias internas, ou, em sua falta, por pessoas e áreas que não tenham responsabilidade com gestão direta da proteção de dados pessoais e privacidade.

Dessa auditoria poderá resultar, como produto, uma avaliação de interesse legítimo (AIL), para as operações em que esta seja a base para tratamento legítimo; um relatório de impacto à proteção de dados (RIPD), em especial quando a operação envolve tratamento de risco; ou um simples relatório para consumo interno.

Não há sucesso no monitoramento sem comunicação clara e precisa sobre as métricas, monitoramento e atividades de auditoria, gerando a devida conscientização interna e externa sobre o programa de privacidade.

Assim, garante-se também a flexibilidade para responder às mudanças no ambiente interno e externo à OSC.
Recomenda-se que a auditoria externa seja realizada de acordo com os ciclos de longo prazo do planejamento da OSC; na falta de planejamento formal de longo prazo, recomenda-se realizar auditoria externa em prazo não menor que três anos e não maior que cinco anos.

4. O caso das OSCs de pequeno porte

Tantas obrigações e deveres podem parecer excessivos para uma OSC de pequeno porte, cujas atividades de tratamento de dados quase sempre se resumem ao seu setor de pessoal e a um website. A ANPD, atenta à situação, publicou em 27 de janeiro de 2022 a Resolução CD/ANPD nº 2, que regulamentou o tratamento de dados por agentes de tratamento de pequeno porte.

Quem pode ser considerado "agente de tratamento de pequeno porte"? Microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos (nos termos da legislação vigente), bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador (Resolução CD/ANPD nº 2, art. 2º, I).

4.1. OSC de pequeno porte e o encarregado pela proteção de dados

Pela Resolução CD/ANPD nº 2, a indicação de encarregado por agentes de tratamento de pequeno porte não é obrigatória; apesar disso, será considerada política de boas práticas e governança, e conta positivamente na avaliação da aplicação de sanções pela ANPD nos casos comprovados de tratamento irregular de dados.

As OSCs que não indicarem encarregado precisam disponibilizar canal de comunicação com o titular de dados para aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências. A melhor forma é indicar no website da organização, junto com seu aviso de privacidade e cookies, um e-mail específico para o tema, indicando o nome completo e o cargo da pessoa a quem titulares de dados pessoais devem se dirigir para exercer seus direitos.

4.2. OSC de pequeno porte e o programa de governança em proteção de dados

Pela Resolução CD/ANPD nº 2, agentes de tratamento de pequeno porte não são obrigados a estruturar um programa de governança em proteção de dados mais elaborado e abrangente. Só precisam adotar medidas administrativas e técnicas essenciais e necessárias, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento.

Se a ANPD verificar tratamento irregular de dados na organização, a comprovação do atendimento às recomendações e às boas práticas de prevenção e segurança divulgadas pela ANPD, inclusive por meio de guias orientativos, será considerada como observância da adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados.

As OSCs de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Essa política deve levar em consideração os custos de implementação, bem como a estrutura, a escala e o volume das operações do agente de tratamento de pequeno porte. Deve, também, prever a adoção de medidas administrativas e técnicas essenciais e necessárias, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento.

Como implementar essa política simplificada de segurança da informação? A própria ANPD fornece, em seu website, um manual intitulado Checklist de medidas de segurança para agentes de tratamento de pequeno porte. A OSC poderá escolher entre implementar por conta própria as medidas indicadas nessa checklist ou – o que é mais recomendado – contratar uma assessoria especializada em adequação à LGPD, que a auxiliará a identificar seu perfil, a diagnosticar as operações de tratamento de dados realizadas pela organização, e a adequá-las à checklist.

O atendimento às recomendações e às boas práticas de prevenção e segurança presente nessa checklist será considerado como observância da adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados.

4.3. Exceção: tratamento de risco

Existem exceções às regras da Resolução CD/ANPD nº 2; para uma OSC, a mais importante é o tratamento de alto risco, ou seja, aquele que atende pelo menos um dos critérios gerais e um dos critérios específicos previstos no artigo 4º da Resolução CD/ANPD nº 2:

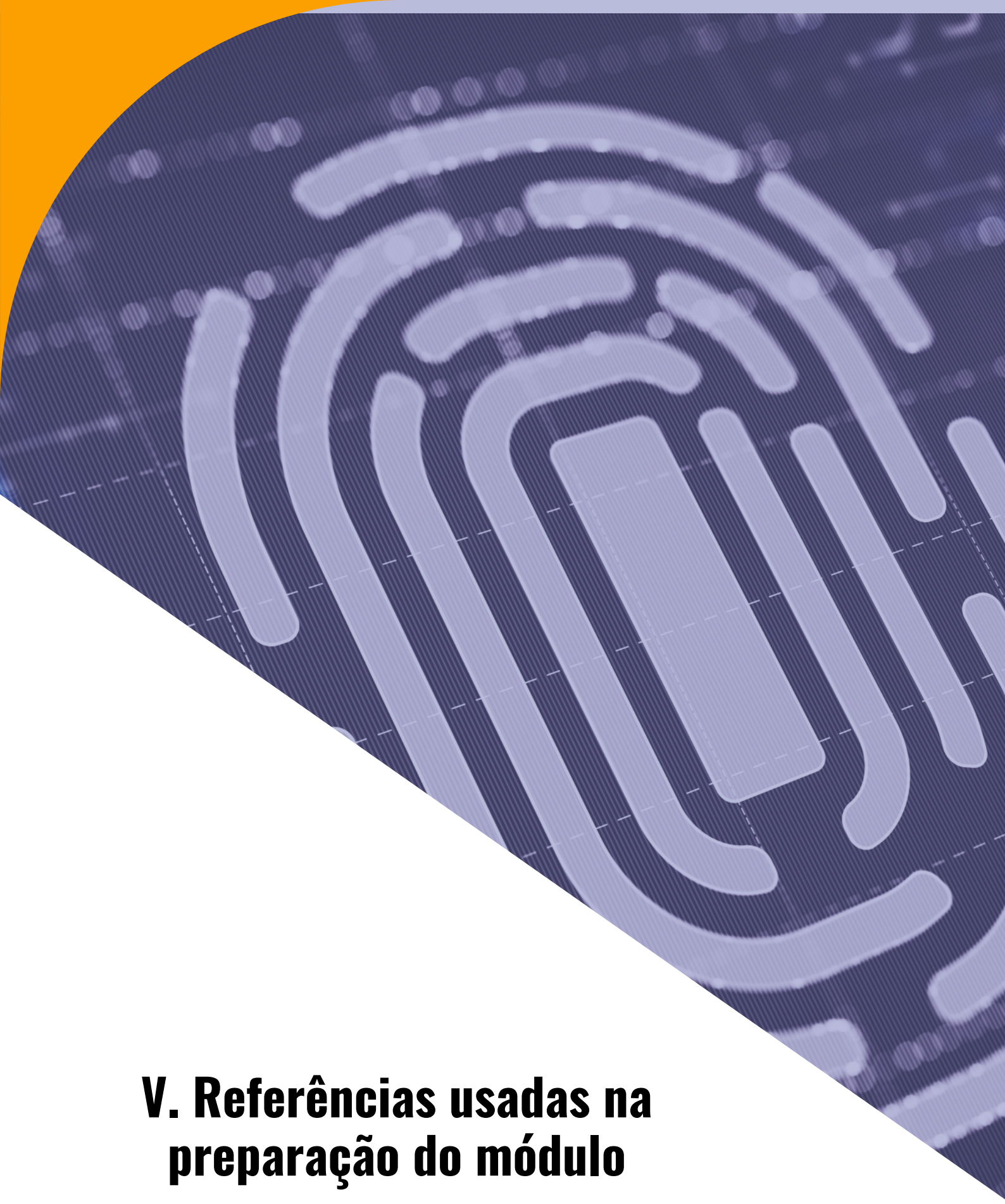
• Critérios gerais: tratamento de dados pessoais em larga escala; ou tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares.

• Critérios específicos: uso de tecnologias emergentes ou inovadoras; vigilância ou controle de zonas acessíveis ao público; decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou a utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

O tratamento de dados de larga escala abrange um número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

Quanto ao tratamento que afete significativamente interesses e direitos fundamentais dos titulares, deve-se observar se a atividade de tratamento impede o exercício de direitos ou a utilização de um serviço, ocasionando danos materiais ou morais aos titulares (discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade).

Se a OSC faz operações de tratamento de dados de alto risco, deve obrigatoriamente indicar um encarregado de proteção de dados e construir um programa de governança em proteção de dados, monitorável periodicamente.



V. Referências usadas na preparação do módulo

- BORELLI, Alessandra; ZAMPERLIN, Emelyn. A importância da conscientização do tema privacidade e proteção de dados nas empresas. Em: BLUM, Renato Opice; WAINZOF, Rony; MORAES, Henrique Fabretti (coords.). **Data protection officer (encarregado)**: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Revista dos Tribunais, 2020. p. 363-386.

- BRUNO, Marcos Gomes da Silva. Monitoramento do programa de privacidade. Em: BLUM, Renato Opice (org.). **Proteção de dados**: desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020. p. 195-207.

- FABRETTI, Henrique; LÓPEZ, Nuria. Frameworks de privacidade na construção de programas de conformidade. Em: BLUM, Renato Opice; WAINZOF, Rony; MORAES, Henrique Fabretti (coords.). **Data protection officer (encarregado)**: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Revista dos Tribunais, 2020. p. 73-84.

- FERREIRA, Raissa Moura; CABELLA, Daniela Motta Monte Serrat. Escrevendo e implantando os avisos de privacidade (privacy notices), na coleta do consentimento válido. Em: BLUM, Renato Opice; WAINZOF, Rony; MORAES, Henrique Fabretti (coords.). **Data protection officer (encarregado)**: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Revista dos Tribunais, 2020. p. 135-150.

- FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de compliance e das políticas de proteção de dados. Em: FRAZÃO, Ana; CUEVA, Ricardo Villas Boas (org.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Revista dos Tribunais, 2021. p. 33-64.

- GASPAR, Marcelo; FIELDER, Viviane. **Data protection officer DPO**: Lei de Proteção de Dados Pessoais. Porto Alegre: PLUS/Simplíssimo, 2020.

- LOPES, Alan Moreira. **Direito Digital e LGPD na prática**. Leme: Rumo Jurídico, 2021.

- MALDONADO, Viviane Nóbrega. Avisos de privacidade e legal design. Em: BLUM, Renato Opice (org.). **Proteção de dados**: desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020. p. 169-180.

- MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; BORELLI, Alessandra (coords.). **LGPD – Lei Geral de Proteção de Dados comentada**. São Paulo: Thomson Reuters Revista dos Tribunais, 2021.

- WIMMER, Miriam; PIERANTI, Octavio Penna. Programas de compliance e a LGPD: a interação entre autorregulação e a regulação estatal. Em: FRAZÃO, Ana; CUEVA, Ricardo Villas Boas (org.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Revista dos Tribunais, 2021. p. 205-224.

VI. Bibliografia complementar para resolver problemas e pensar em novas ideias!

- A guide to privacy by Design. Agência Espanhola Proteción Datos

ACESSE

- Segurança da informação para agentes de tratamento de pequeno porte – Guia orientativo (ANPD)

ACESSE

- Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado (ANPD)

ACESSE

- Vazamento de dados – cartilha de segurança para a internet (ANPD)

ACESSE

- Proteção de dados – cartilha de segurança para a internet (ANPD)

ACESSE

- Cookies e proteção de dados pessoais – guia orientativo (ANPD)

ACESSE

- Tratamento de dados pessoais no Poder Público – guia orientativo (ANPD)

ACESSE

- Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral – guia orientativo (ANPD)

ACESSE

- O terceiro setor no Brasil e a LGPD (Consultor Jurídico)

ACESSE

- A flexibilização da LGPD e o terceiro setor (Consultor Jurídico)

ACESSE

- Programas corporativos de privacidade (Data Privacy Brasil)

ACESSE

- LGPD no terceiro setor: principais desafios (OAB-MG)

ACESSE

- Manual de adequação à LGPD para organizações da sociedade civil do IDEC

ACESSE

Guia de Conformidade Legal para Organizações da Sociedade CIvil

Página de Publicações da Autoridade Nacional de Proteção de Dados pessoais

Site e Canal do Youtube do Data Privacy Brasil

Site do CERT.Br (Centro de Estudos, Resposta e Tratamento de Incidentes de segurança no Brasil)

Projeto LGPD nos tribunais - para entender o contencioso sobre o tema

O Papel do/a encarregado/a conforme a Lei Geral de Proteção de Dados Pessoais (LGPD)

AS 12 PRINCIPAIS PRIORIDADES ORGANIZACIONAIS PARA A IMPLEMENTAÇÃO EFICAZ DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

VI. Anexos

Modelo mapeamento

ACESSE

Modelo de política de privacidade

ACESSE

Modelo teste legitimo interesse

ACESSE

Modelo resposta incidente

ACESSE

Modelo cláusulas de proteção de dados pessoais

ACESSE

Modelo de política de privacidade para trabalhadores e prestadores de serviço

ACESSE

EXPEDIENTE ELO:

Diretoria - 2024-2026
Maria Elisa Huber Pessina - Coordenadora Geral
Rebeca Ribas Bulhosa - Tesoureira
Maria Ubajareida Carvalho Frota - Secretária
Ute Emma Gertrud Engelke (suplente)

Conselho Fiscal
Elen Catarina Santos Lopes
Louisa Huber
José Augusto Laranjeiras Sampaio
Damien Marie Jean Hazard (suplente)

Demais Associadas/os
Caroline Almeida
Claudete Mary Souza Alves
Eliana Bellini Rolemberg
Elsa Sousa Kraychete
Émerson Fontinele de Barro
Gabriel Kraychete
José Maurício Carneiro Daltro Bittencourt
Luana Vilutis
Maria de Fátima Pereira do Nascimento
Omar da Rocha Júnior
Renata Silva Jesus

Equipe ELO:
Camila Veiga - Coordenadora Executiva
Candice Araújo - Assessora
Cristina Costa - Assistente Adm-Financeiro
Elza Montal - Assessora de Comunicação
Fátima Nascimento - Consultora Associada
Eliana Rolemberg - Consultora Associada

FICHA TÉCNICA:

Organização:
Fátima Nascimento

Textos:
Fátima Nascimento; Aline Viotto e Laura Arantes;
Maraísa Rosa Cezarino;
Manuel Nascimento;

Layout e diagramação:
Elza Montal

Correção ortográfica:
Taliane Oliveira

As imagens utilizadas nesta publicação são provenientes de bancos de imagens licenciados e estão em conformidade com a legislação vigente, incluindo as normas estabelecidas pela Lei Geral de Proteção de Dados (LGPD).