GUIA DE

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

AO TERCEIRO SETOR

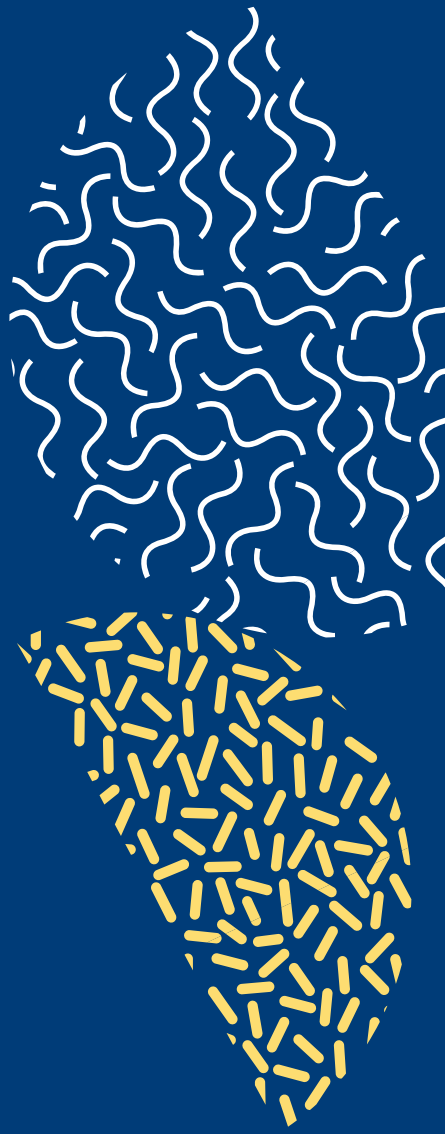
JULHO DE 2022

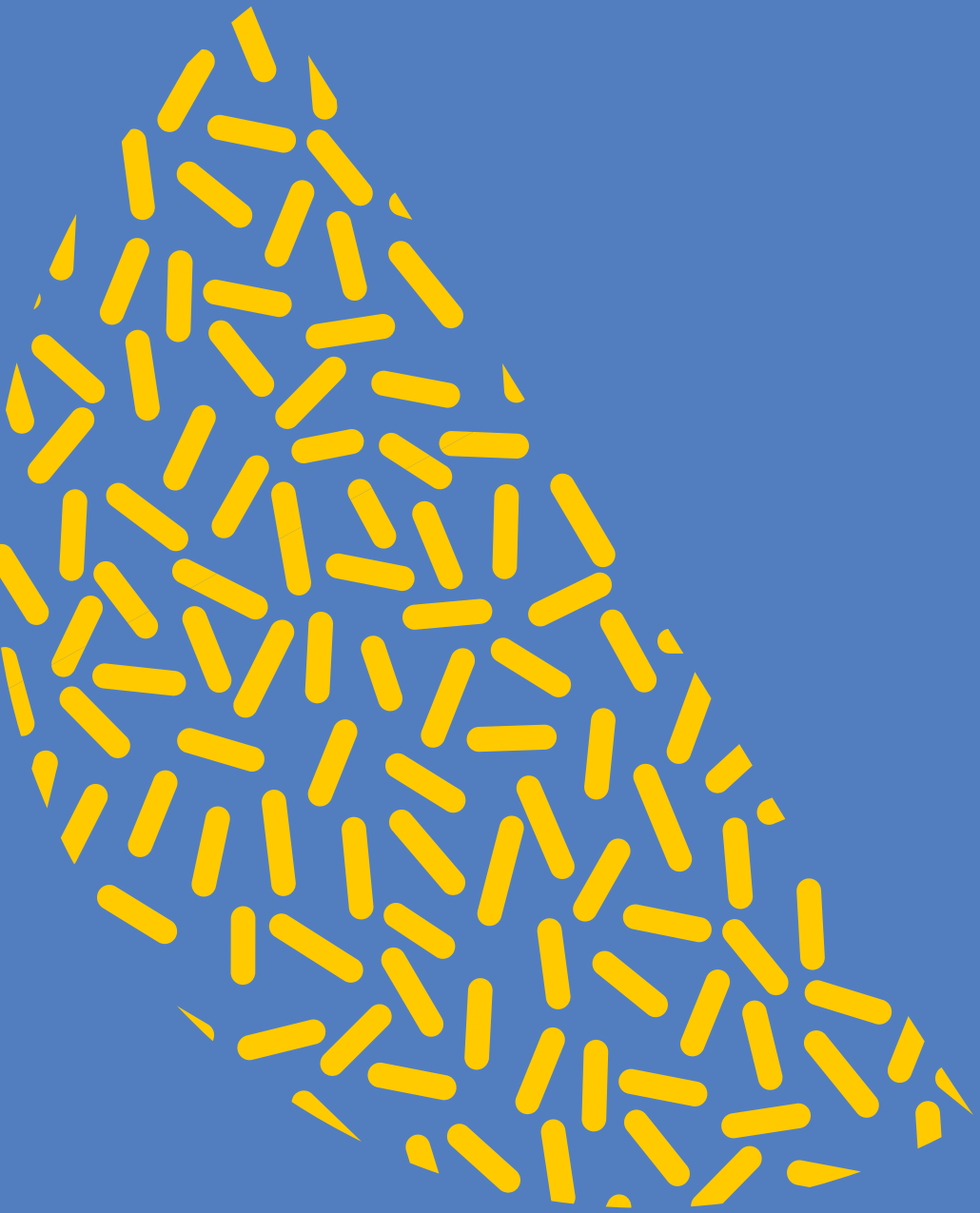
b/luz

Instituto Ayrton Senna

Índice

Índice clicável





Elaboração:

Adriane Loureiro Novaes

Odélio Porto Junior

Matheus Botsman Kasputis

Luiz Felipe Sundfeld Ibrahim

Rafaela Sobrinho Marcondes

Fernanda Catão de Carvalho

Revisão:

Fernando Bousso

Marina Beividas

Samira V Miguel

Projeto Gráfico:

Fernanda Muchon

Laura Klink

Voltar para o índice

Introdução

O Brasil, seguindo uma tendência mundial de regulação do uso de dados pessoais[1], aprovou em agosto de 2018 a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), exigindo que as organizações revisem suas práticas e adaptem seus processos relacionados ao tratamento/processamento[2] de dados pessoais.

A LGPD é aplicável a todos os setores da economia, incluindo as instituições do terceiro setor, que são grandes mobilizadoras de iniciativas para impulsionar o desenvolvimento social e, para atingir esse objetivo nos dias atuais, é imprescindível o uso de dados pessoais.

Dado Pessoal

É qualquer informação/dado que **identifique diretamente** uma pessoa física (p. ex. nome completo, documento de identificação oficial etc.), ou que **torne uma pessoa identificável** (p. ex. nº de registro de um empregado ou doador, histórico de doações etc.).

[1]Neste guia, os termos "dados pessoais" e "dados" são utilizados de forma intercambiável, mas é importante esclarecer que a LGPD somente se aplica ao uso de dados pessoais.

[2]Neste guia, os termos referentes ao uso de dados pessoais "tratamento" e "processamento" são utilizados de forma intercambiável. A LGPD utiliza somente o termo "tratamento", definindo-o de forma ampla como qualquer tipo de uso de dados pessoais (art.5, X, da LGPD): "X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Sobre este Guia

Este guia foi desenvolvido pelo Instituto Ayrton Senna, em parceria com o escritório Baptista Luz Advogados, e busca apresentar pontos de atenção e aspectos da LGPD relevantes às entidades que fazem parte do terceiro setor. Este guia foi elaborado em fevereiro de 2022, tem um caráter meramente informativo e não substitui nem deve ser entendido como aconselhamento jurídico.

Com isso em mente, o presente guia busca apresentar os riscos das práticas realizadas pelo terceiro setor, bem como possíveis melhorias que possam ser implementadas nas atividades do dia a dia dessas instituições. Além disso, o presente guia fornece um conjunto simples de etapas que tais instituições podem seguir para se adequarem à LGPD, evitando multas e permanecendo com boa reputação no mercado.

Também abordaremos neste guia aspectos importantes sobre o tratamento de dados pessoais de crianças e adolescentes, tema bastante relevante para o universo de boa parte das organizações do terceiro setor. Sobre esse aspecto, importante destacar que o Estatuto da Criança e do Adolescente (ECA) define juridicamente "criança" como a pessoa até doze anos de idade incompletos e "adolescente" como a pessoa entre doze e dezoito anos de idade[3].

[3]Art. 2 da Lei nº 8.069/1998.

Voltar para o índice

2 Principais atividades de tratamento de dados pessoais conduzidas pelo terceiro setor

De acordo com a LGPD, todo tratamento de dados pessoais deve se valer de uma base legal[4] válida e adequada para justificá-lo. A lei estabelece diversas bases legais que podem autorizar um tratamento de dados, sendo o consentimento[5] apenas uma delas. E como isso se aplica para o terceiro setor? Quais são os impactos da LGPD para as principais atividades de tratamento conduzidas por tais entidades?

A seguir analisamos 4 dessas principais atividades:

[4]base legal: hipótese prevista em lei que autoriza o tratamento de dados pessoais.

[5]consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

2.1. Marketing

As atividades de marketing estão presentes de maneira relevante no terceiro setor, seja para a captação de recursos, seja para a promoção dos fins sociais perseguidos pela organização. Tais atividades costumam envolver a criação de listas com grandes volumes de dados pessoais, abrangendo, ao menos, informações como nome, telefone e endereço de e-mail de doadores ou contribuintes.

Para o terceiro setor, importante também ressaltar a prevalência do chamado marketing social, pelo qual as organizações promovem causas, projetos e objetivos direcionados à sociedade.[6] Vale destacar que a LGPD também se aplica a esses casos, mesmo não havendo tratamento de dados para fins exclusivamente comerciais, devendo suas regras e princípios serem observados. Para isso é possível fundamentar-se na base no **legítimo interesse da organização ou de terceiros**.

[6]V. LEVY, Sidney; KOTLER, Philip, Broadening the Concept of Marketing, Journal of Marketing, n. 1, v. 33, p. 05-10, jan - fev, 1969.

Saiba mais sobre o legítimo interesse

O legítimo interesse é uma base legal que não depende da autorização do titular para que uma entidade possa utilizar seus dados. Para que essa base possa justificar um tratamento de dados, é necessário que o tratamento tenha uma finalidade legítima e que haja algum nível de expectativa do titular em relação ao tratamento de seus dados.

Por isso, ao valer-se do legítimo interesse, medidas de transparência e o cumprimento dos princípios da LGPD devem ser reforçados pela organização. Além disso, especialmente quando existir incerteza sobre o uso dessa base legal, é recomendável a elaboração de um **teste de legítimo interesse** (conhecido como legitimate interest assessment – LIA) para se verificar a possibilidade de sua aplicação, ante os possíveis riscos oferecidos ao titular, e os eventuais mitigadores de risco que podem ser adotados, além de documentar essa escolha.

A aplicabilidade do legítimo interesse depende de uma análise holística do caso concreto. Por exemplo, o envio de e-mail marketing a atuais ou antigos doadores pode se enquadrar na base legal do legítimo interesse, devido à pré-existência de um relacionamento do titular dos dados com a organização, o que reforça a expectativa do titular. Por outro lado, o envio de comunicações com base no legítimo interesse para pessoas sem relacionamento prévio com a organização deve ser analisado com mais cautela; embora não seja proibido pela LGPD, o envio de comunicações de marketing para esse público deve ser previamente avaliado por meio de um balanceamento entre eventuais riscos aos titulares e os interesses da organização.

Em qualquer caso, deve-se fornecer ao titular a opção de interromper o recebimento de comunicações (opt-out) a qualquer momento e de forma facilitada.

Na maioria dos casos, fica a critério da organização a escolha entre o consentimento ou o legítimo interesse, a depender da característica da campanha conduzida. Alguns fatores podem ser considerados no momento da decisão:

Legítimo interesse

/ Independe de consentimento, podendo o tratamento ser iniciado **imediatamente**

/ Tem a capacidade de atingir um **público-alvo maior**

/ Deve **balancear** os interesses da organização com os direitos e as liberdades do indivíduo

/ **Não pode** ser utilizado para o tratamento de dados pessoais sensíveis e dados de crianças

/ O titular dos dados pessoais terá o direito de se **opor mais facilmente ao tratamento**

/ Em certos casos, pode ser questionável quando a **expectativa dos titulares for menor**

Consentimento

/ O tratamento dos dados somente pode ser iniciado **após** a manifestação de vontade do indivíduo

/ Possivelmente atingirá um **público-alvo menor**, limitado apenas àqueles que consentiram

/ Deve ser **livre, informado, inequívoco** e para finalidades determinadas, devendo ser registrado[7]

/ **Pode** ser utilizado para o tratamento de dados pessoais sensíveis e dados de crianças, desde que o consentimento de pelo menos um dos pais ou responsável legal seja obtido de forma destacada

/ O titular dos dados pessoais terá o direito de **revogar o consentimento**

/ Garante uma real **liberdade de escolha** ao indivíduo quando observados seus requisitos

[7] o consentimento deve refletir as vontades do titular, ser obtido por meio de uma ação afirmativa, estar separado de outros termos e condições e ser fruto de uma livre escolha, passível de revogação.

/ Publicidade personalizada

Buscando maior eficiência, as organizações podem optar por estratégias de publicidade personalizada, criando listas de pessoas com interesses específicos em determinados setores de atuação. Em maior ou menor grau, a publicidade personalizada envolve a criação de perfis comportamentais (profiling), o que, pela técnica empregada e o volume de dados utilizado, pode agravar o risco da atividade de tratamento.

A publicidade personalizada, no entanto, continua sendo uma prática utilizada de maneira crescente no mercado, e que convive em harmonia com o ecossistema de proteção de dados pessoais brasileiro, desde que observados os princípios e as regras gerais da LGPD.

/ Listas frias[8] e enriquecimento de dados[9]

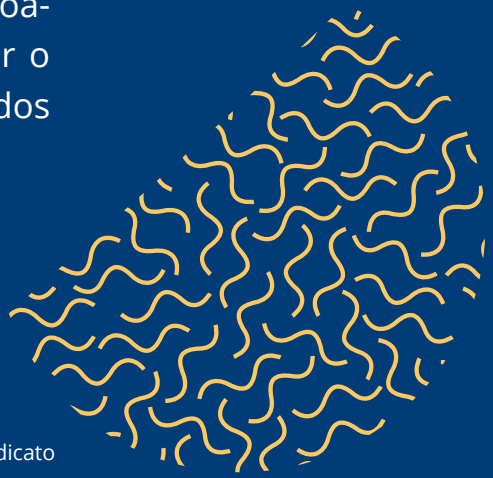
Outra situação comum no segmento de marketing é a **compra de listas frias e o enriquecimento de bases de dados**. Embora tais atividades não sejam proibidas pela LGPD, devem ser observadas com muita cautela, pois podem representar às organizações riscos não apenas jurídicos, mas também operacionais. Diante disso, deve-se atentar à procedência das bases de dados adquiridas de terceiros para que não sejam tratadas informações falsas, imprecisas ou obtidas em desconformidade com a lei (por exemplo, sem uma base legal válida). Com maior efeito, tais atividades podem ainda contaminar bases de dados já existentes e prejudicar os objetivos da organização.

[8]Listas frias: no presente caso, trata-se de listas de pessoas que não são doadores da organização, mas podem vir a ser, ou seja, são potenciais doadores.
[9]Enriquecimento de dados: em termos gerais, enriquecimento de dados é a prática pela qual uma organização adiciona mais informações aos dados que já possui sobre um indivíduo, permitindo, por exemplo, uma publicidade mais direcionada ou o contato com o titular dos dados.

Atenção aos Dados de Crianças e aos Dados “Sensíveis”

Importante reforçar que, se a atividade de marketing envolver dados sensíveis[10] ou dados de crianças, será necessário o consentimento, não podendo a organização se valer do legítimo interesse. Imagine, por exemplo, uma entidade do terceiro setor atuante no segmento de saúde que, conhecendo determinados doadores portadores de câncer, decide enviar-lhes comunicações sobre novos tipos de tratamentos oncológicos conduzidos por um hospital parceiro.

Nesse caso, a formação de uma lista de e-mail marketing com este público deverá acompanhar o consentimento específico e destacado de cada doador, uma vez que as informações de saúde utilizadas para selecionar o público-alvo (como o quadro clínico) enquadram-se na categoria de dados sensíveis.



[10]dado pessoal sensível: 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.

/ Cuidados nas atividades de marketing

Para garantir que as atividades de marketing exercidas estejam de acordo com a LGPD, vale se atentar às seguintes recomendações:

/ Garanta que os titulares possam optar por não receber suas comunicações de marketing e que sejam devidamente avisados sobre isso. Por exemplo, coloque um botão de descadastro ao final das comunicações de marketing.

/ Respeite os direitos do titular, dando acesso facilitado às informações sobre o tratamento de dados, utilizando-os somente para as finalidades autorizadas e guardando os dados com segurança.

/ Não adicione automaticamente pessoas à sua lista de e-mails caso não tenha feito um contato inicial ou tenha uma relação pré-existente sem avaliar o caso concreto com os responsáveis por privacidade na organização.

/ Não compre mailings e listas de contatos, se não tiver base legal legítima e adequada para tanto. O ideal é que sempre seja feita uma análise dos fornecedores e parceiros à LGPD, visando avaliar o nível de adequação desses terceiros à LGPD e a legitimidade da origem dos dados pessoais obtidos.

/ Quando optar pelo consentimento, obter tal consentimento por meio de uma autorização livre, informada e inequívoca, que deve ser registrada.

/ Quando optar pelo legítimo interesse, avaliar a necessidade de elaboração de um teste de legítimo interesse a fim de harmonizar os interesses da organização com os direitos e liberdades do titular.

/ Não use checkboxes pré-marcados quando a atividade se valer do consentimento - isso não constitui consentimento válido e pode confundir o titular.

/ Não opte pelo legítimo interesse quando a atividade envolver dados de crianças ou dados sensíveis.

2.2. Arrecadação de recursos

A arrecadação ou captação de recursos pode ocorrer de várias formas no terceiro setor. Sob o ponto de vista de proteção de dados, a mais relevante é aquela realizada por meio de doação. Hoje, muitas transações são celebradas pela internet, valendo-se as organizações de formulários eletrônicos e meios de pagamento online. As organizações também podem firmar patrocínios ou parcerias com o setor privado, como por meio de programas de salary donation[11] – conforme será descrito a seguir.

Tendo em vista a natureza da relação com o doador, a base legal adequada para o uso de dados pessoais para a arrecadação de recursos será a **execução de contrato ou procedimentos preliminares**, ainda que não tenha sido formalizado um contrato, mas apenas tenha sido realizado um depósito ou o preenchimento de um formulário. Tal base legal abrangerá não apenas as informações coletadas em fichas ou formulários de doação para que seja processado o pagamento, mas também a gestão do relacionamento com o doador quando tal atividade for necessária para a execução do contrato como, por exemplo, emissão de notas fiscais, prestação de contas e serviços de atendimento.

As doações feitas por formulários eletrônicos devem observar as melhores práticas para garantir conformidade com a LGPD, que podem incluir:

[11]salary donation: significa a doação descontada automaticamente do salário de funcionários de uma empresa parceira da organização.

- Menção prévia à **política de privacidade** e ao **aviso de cookies** da organização.
- Coleta apenas dos **dados necessários** (relevantes, não excessivos e proporcionais) para a celebração da doação.
- Descrição da **finalidade** da coleta de cada dado pessoal solicitado no formulário caso não esteja muito claro (como por meio de just-in-time notices[12]).
- Uso de **cores** contrastantes e **fontes** em tamanho legível, evitando a indução de determinados comportamentos do titular dos dados (p. ex. dark patterns[13]).

A organização que celebra parcerias com empresas do setor privado e organiza, por exemplo, programas de apoio à organização por meio de recursos oferecidos pelos próprios empregados da empresa, que doam uma parte de seus salários, também poderá se aproveitar da execução de contrato como base legal adequada. Neste caso, o funcionário que concordar com o débito mensal automático de parcela da sua remuneração, em folha de pagamento, para fins de doação, pode ter seus dados compartilhados diretamente pelo empregador do funcionário com a organização.

[12] Just-in-time notices são pop-ups ou legendas que surgem, a partir de certas interações, comumente em formulários eletrônicos, a fim de explicar como determinada informação fornecida pelo titular dos dados será utilizada pelo agente de tratamento. É o caso de esclarecer, por exemplo, que a coleta do CPF do titular tem como propósito prevenir fraudes, como falsidade ideológica.

[13] Dark patterns são elementos de design utilizados para manipular comportamentos ou induzir o usuário ao erro, a fim de, a detrimento do titular, beneficiar o provedor de um serviço ou o fornecedor de um produto.

Posso enviar publicidade com os dados obtidos no formulário de doação?

Neste caso, de maneira geral, aplicam-se as mesmas regras mencionadas no **item 2.1** acima, podendo a organização valer-se do consentimento ou do legítimo interesse. No entanto, caso a organização pretenda aproveitar-se dos dados obtidos no formulário de doação para o envio de comunicações publicitárias, deverá assumir alguns cuidados, considerando que tais comunicações serão consideradas uma **finalidade secundária** à doação.

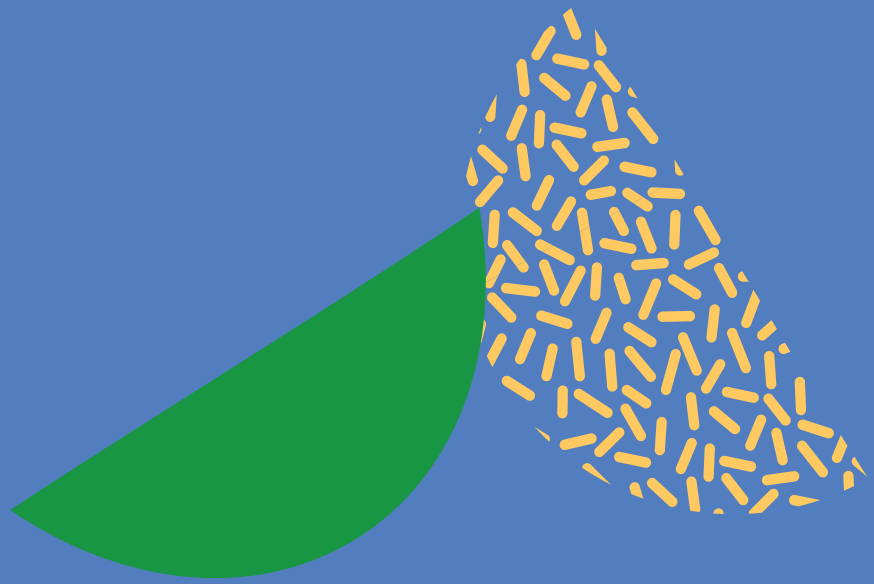
Optando a organização pelo consentimento, deverá providenciar um **checkbox** ao titular dos dados para que este concorde com o envio de comunicações publicitárias sobre os projetos e objetivos da organização. Para que haja uma manifestação de vontade livre, o checkbox não poderá estar pré-marcado, uma vez que neste caso não é admitido pela LGPD um consentimento tácito.[14]

Optando a organização pelo legítimo interesse, deverá providenciar no formulário um **texto informativo**, mencionando que os dados utilizados para a doação poderão ser aproveitados para o envio de publicidade pela organização, destacando também que o titular dos dados terá o direito de se opor ao recebimento de tais mensagens (opt-out).

Em ambos os casos, os dados coletados exclusivamente para fins publicitários – e que não forem necessários para a doação – devem ser de fornecimento opcional pelo titular dos dados, simbolizados, por exemplo, com um asterisco ou uma explicação entre parênteses. Isso é importante para que a doação não esteja condicionada ao envio de publicidade, prejudicando a autonomia do titular.

[14]consentimento tácito: significa que a manifestação da vontade do titular ocorreu de forma implícita

Importante ressaltar que a organização não deverá aceitar da empresa parceira dados excessivos ou inadequados para as finalidades principais ou acessórias à doação. Deverá haver previsão expressa sobre o programa em contrato de patrocínio ou similar, acompanhado de cláusulas robustas de privacidade e proteção de dados pessoais que definam, entre outros, a finalidade do tratamento, os dados pessoais envolvidos e as medidas de segurança aplicadas.



/ Cuidados na arrecadação de recursos

Os seguintes cuidados devem ser considerados pelas organizações ao conduzirem atividades de arrecadação de recursos:

/ **Garanta** transparência ao titular com hiperlinks nos formulários de doação, inclusive os eletrônicos, direcionando à política de privacidade ou ao aviso de privacidade.

/ **Compatibilize finalidades adicionais** de tratamento de dados (como envio de publicidade) com os propósitos iniciais da coleta das informações, valendo-se de checkbox ou texto informativo, dependendo da base legal adotada.

/ Inclua disposições específicas sobre privacidade e proteção de dados em **contratos celebrados** com empresas parceiras ou com o titular dos dados, quando aplicável.

/ **Não colete informações excessivas ou desnecessárias** do titular nos formulários de doação, inclusive eletrônicos.

/ **Não utilize os dados para finalidades adicionais** sem informar devidamente o titular das informações e avaliar, no caso concreto, a adequação desse tratamento.

/ **Não deixe de avaliar o parceiro e o fornecedor** em relação aos aspectos de proteção de dados. A LGPD aplica responsabilidade solidária[15] aos agentes de tratamento[16] que estejam diretamente envolvidos no tratamento do qual decorreram danos ao titular, ou seja, ambos os agentes de tratamento serão responsáveis por tais danos, salvo em determinadas hipóteses.

[15] Responsabilidade solidária, neste contexto, significa que ambos os agentes (controlador e operador) podem ser responsáveis, em conjunto, pelo tratamento de dados pessoais. Em outras palavras, o tratamento de dados pessoais gera efeitos em toda a cadeia, podendo responsabilizar todas as partes envolvidas.

[16] A LGPD define o termo "agente de tratamento" como pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais ("Controlador") ou a quem compete tratar os dados pessoais em nome de um controlador ("Operador"). Ver art. 5º da LGPD.

2.3. Uso de imagem

Pode ser comum na rotina da organização o uso gratuito ou remunerado da imagem de seus colaboradores ou doadores para eventual promoção das atividades e objetivos da organização. Nesse sentido, a legislação e a jurisprudência exigem a autorização específica da pessoa retratada, o que pode ser obtido por um **termo de autorização de uso de imagem**.[17]

Embora o direito de imagem seja autônomo em relação ao direito à proteção de dados, a imagem do titular registrada em foto ou vídeo é indissociável do caráter de dado pessoal, de modo que o **consentimento** para uso de imagem pode ser aproveitado no contexto do tratamento de dados, principalmente nos casos em que o direito de uso da imagem é concedido a título gratuito. Nesse caso, importante respeitar os princípios da LGPD para uma manifestação de vontade livre, informada e inequívoca, bem como, no que couber, o direito de revogação do consentimento do titular dos dados.

[17]Conforme o Código Civil: "Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. (Vide ADIN 4815)".

Vale destacar que a necessidade de consentimento pode ser relativizada em situações excepcionais, principalmente quando não houver a individualização da pessoa, sendo ela retratada, por exemplo, diante de um grupo de pessoas ou por uma pequena fração de tempo.[18] Tais hipóteses devem ser interpretadas restritivamente, sobretudo quando a pessoa retratada for uma criança ou adolescente, já que nessa situação deve haver autorização do pai ou responsável legal para a veiculação da imagem, tendo em vista as regras do Estatuto da Criança e do Adolescente.[19]

Em todo caso, sempre que possível, recomenda-se que seja obtido o consentimento do retratado. Além disso, é importante que o termo de autorização de uso de imagem defina com precisão, entre outros, os seguintes aspectos:

[18]STJ. REsp 1772593/RS. Relator(a): Ministra Nancy Andrighi. Terceira Turma. DJ 16.06.2020. DJe 19.06.2020.

[19]Arts. 17, 18 e 100, inciso V, do Estatuto da Criança e do Adolescente (Lei n. 8.069/1990).

- a finalidade do uso da imagem, sugerindo-se a menção expressa à utilização para fins sociais quando for o caso.
- as condições de uso da imagem, inclusive quanto à gratuidade ou remuneração da concessão de uso.
- as formas de exposição da pessoa retratada (p. ex. gravações de vídeo para produção artística, redes sociais, imagens em website etc.).

O uso de imagem sem autorização do retratado ou para finalidade incompatível com a autorização pode sujeitar a organização à responsabilização por danos morais. Ressalta-se, ainda, que o uso não autorizado para fins comerciais ou econômicos independe de prova do prejuízo perante o judiciário.[20]

[20]Conforme a Súmula n. 403 do STJ: "Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais".

/ Cuidados no uso de imagem

Os seguintes cuidados devem ser considerados pelas organizações ao conduzirem campanhas ou ações com a utilização de imagem:

/ **Obtenha a autorização da pessoa retratada** para a concessão de uso do direito de imagem, com detalhamento específico das condições em que a imagem será utilizada em um termo de autorização de uso de imagem.

/ Garanta ao titular dos dados o direito de **revogação de consentimento** no que couber, com menção expressa a possíveis limitações desse direito.

/ Avalie com cautela as hipóteses excepcionais em que a **autorização para o uso da imagem pode ser relativizada**, mas, sempre que possível, como boa prática, busque obter o consentimento da pessoa retratada.

/ Não explore a imagem da pessoa retratada **com termos genéricos ou ambíguos,** sem definir, por exemplo, a finalidade, o prazo, a forma e as condições do uso da imagem.

/ Não estabeleça **condições irrestritas** que limitem de maneira definitiva os direitos da personalidade do indivíduo.

/ Não faça uso da imagem **sem a devida autorização da pessoa retratada** ou sem avaliar, detalhadamente, a possibilidade de dispensa de consentimento.

2.4. Produção de estudos e pesquisas científicas

A produção de estudos e pesquisas científicas também pode permear as atividades das entidades do terceiro setor em seus empreendimentos sociais. A LGPD trata do tema ao definir regras específicas para os órgãos de pesquisa, embora não estabeleça restrições às atividades das organizações que se enquadrem nesse conceito.

De acordo com a definição da LGPD, uma organização pode ser considerada órgão de pesquisa caso tenha como objetivo social, estatutário ou em sua missão institucional a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico, e não possua fins lucrativos[21]. Como órgão de pesquisa, a organização tem a prerrogativa de se valer de uma base legal específica, definida no inciso IV do artigo 7º da LGPD, para conduzir suas atividades para essa finalidade.[22]

[21] Art. 5º da LGPD: "[...] XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico".

[22] "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais". O enunciado foi também reproduzido pelo art. 11, II, "d", aplicável ao tratamento de dados sensíveis.

As organizações que não se enquadrem em tal definição ainda podem tratar dados pessoais para condução de estudos e pesquisas científicas, no entanto, devem se valer de outras bases legais, como o consentimento ou o legítimo interesse.

A LGPD traz ainda regras especiais[23] para os estudos em saúde pública realizados por órgãos de pesquisa, as quais incluem **(i)** a necessidade de anonimização ou pseudonimização[24] dos dados pessoais, e a proibição de divulgar dados pessoais nos resultados ou excertos do estudo ou pesquisa; **(ii)** tratamento dos dados exclusivamente dentro do órgão e para os fins da pesquisa ou estudo; **(iii)** manutenção dos dados em ambiente seguro e controlado (a partir da adoção de medidas técnicas e administrativas adequadas de segurança da informação e da implementação de controles de acesso para que somente pessoas autorizadas tenham acesso aos dados pessoais), conforme regulamento específico; **(iv)** respeito aos padrões éticos do setor.

Ainda quanto às pesquisas na área da saúde, no contexto específico de pesquisas envolvendo seres humanos, vale reforçar as recomendações do Conselho Nacional de Saúde no sentido de que, além da necessidade de obtenção do Termo de Consentimento Livre e Esclarecido (TCLE), exigido pela Resolução n. 466/2012 do CNS, o órgão de pesquisa deverá garantir a confidencialidade e a anonimização dos dados antes do encaminhamento a qualquer patrocinador ou a terceiros.[25]

Em se tratando da realização de estudos e pesquisas científicas com crianças, recomenda-se a obtenção do consentimento de um dos responsáveis legais para o tratamento dos dados. O tratamento anonimizado das informações também é recomendável durante todo o processo, principalmente na publicização dos resultados, conforme as sugestões do **item 4.1** deste guia.

[23]Art. 13 da LGPD.
[24]Para entendimento dos conceitos de anonimização e pseudonimização, veja a página 50 deste Guia.
[25]Conselho Nacional de Saúde. **Manual de Orientação: Pendências Frequentes em Protocolos de Pesquisa Clínica**, p. 24, 2015. Disponível em <https://bityli.com/0USPI>. Acesso em 23/08/2021.

/ Cuidados na condução de pesquisas e estudos

Os seguintes cuidados devem ser considerados pelas organizações ao conduzirem pesquisas ou estudos científicos:

/ Verificar a necessidade da obtenção de **consentimento** do titular dos dados, sobretudo nos casos de pesquisas na área da saúde ou com crianças.

/ Sempre que possível **anonimize** ou, ao menos, **pseudonimize** as informações tratadas quando do compartilhamento com outras áreas da organização ou com terceiros, bem como quando da publicização dos resultados da pesquisa ou do estudo.

/ Garanta a **segurança e a confidencialidade** dos dados tratados, mantendo-os armazenados em ambientes seguros e controlados, respeitando as normas e os **padrões éticos e bioéticos** setoriais para pesquisas com seres humanos.

/ Não trate dados sem avaliar a **base legal mais adequada para o tratamento**, seja o consentimento, a realização de estudos por órgãos de pesquisa ou o legítimo interesse.

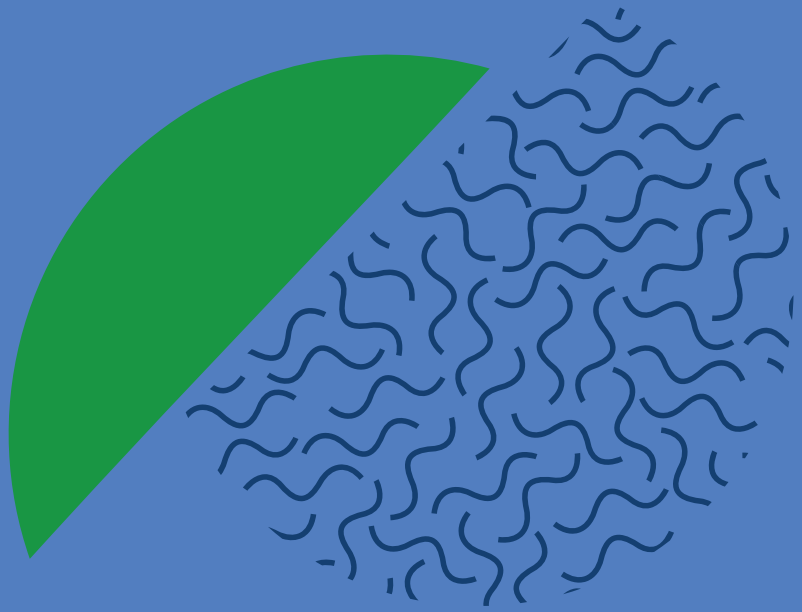
/ Não compartilhe dados pessoais individualizados **quando for possível anonimizá-los** ou, ao menos, **pseudonimizá-los**, para disponibilização em formato agregado e/ou não-identificável.

/ Não trate os dados de **maneira informal**, sem controles de segurança prévios e sem políticas ou procedimentos internos bem definidos.

Voltar para o índice

3 Riscos comuns no uso de dados de crianças e adolescentes

Neste item são elencados os principais riscos à privacidade e à proteção de dados pessoais quando do uso de informações de crianças e adolescentes, a fim de orientar as organizações a melhor mitigar os riscos e/ou evitá-los.



3.1. Desconsideração da Autonomia da Criança ou do Adolescente

Tanto o Estatuto da Criança e do Adolescente[26] quanto a Convenção sobre os Direitos da Criança[27] reconhecem as crianças e adolescentes como sujeitos de direito. Desse modo, o direito à privacidade e à proteção dos dados pessoais, conforme o caso concreto, devem ser implementados buscando-se respeitar a autonomia da criança e do adolescente. Importa ressaltar que o direito à privacidade e à proteção de dados são pré-requisitos para que outros direitos fundamentais possam se desenvolver, como os da liberdade de pensamento, de expressão e do desenvolvimento da personalidade.

Assim, pode haver casos em que a prerrogativa decisória sobre o uso de dados pessoais pode caber predominantemente à criança ou ao adolescente. Nesses casos, o agente de tratamento deve ponderar as limitações da capacidade de compreensão e decisão da criança e do adolescente, equilibrando-as com a sua autonomia e com a busca do seu melhor interesse.

[26] Art. 3º da Lei nº 8.069/1990.

[27] Decreto do Presidente da República nº 99.710/1990.

3.2. Falta de Transparência

Um dos pilares da proteção de dados pessoais é fornecer aos titulares informações claras e adequadas sobre como seus dados serão utilizados. Nesse sentido, deve-se destacar que esse dever se direciona tanto aos pais/responsáveis quanto às próprias crianças e adolescentes.

O direito da criança ou do adolescente a obter informações adequadas à sua compreensão sobre o uso de seus dados ganha destaque, principalmente, nas situações em que eles possuem um papel ativo no fornecimento dos dados. Exemplo comum são os casos de aplicativos desenvolvidos para o uso desse público.

Assim, as crianças e os adolescentes também precisam ser vistos como sujeitos de direitos, devendo ter seus direitos como titulares dos dados respeitados com base em sua capacidade de compreensão e seu contexto social.[28]

[28]"Quando se trata de privacidade, estudos revelaram que as crianças geralmente consideram ter direito à privacidade online em relação a seus pais ou colegas (ou seja, uma 'privacidade social'), mas têm um entendimento muito menos desenvolvido sobre o fato de que sua privacidade também pode ser violada por atores estatais ou empresas (Livingstone S, 2018; Ofcom, 2008; Zarouali B et al., 2017)." MILKAITE, Ingrida; e LIEVENS, Eva. Children's Rights to Privacy and Data Protecton Around the World: Challenges in the Digital Realm. **European Journal of Law and Technology**, edição nº 1, volume 10. 2019. Disponível em: <https://bit.ly/3z86xxO>. Acesso em: 17/08/2021.

Como fica a transparência na prática?

Uma pesquisa empírica, conduzida em 2010, buscou entender qual é o nível de compreensão de crianças quanto ao conteúdo das políticas de privacidade disponíveis online. A conclusão não surpreendeu. Os participantes apontaram diversos problemas que prejudicaram a interpretação das políticas de privacidade, variando desde a complexidade da linguagem aos elementos do design e de diagramação das páginas.[29]

Diante disso, as autoras destacaram recomendações para melhorar a legibilidade das políticas de privacidade, principalmente diante do público infantil, as quais envolveram, entre outras: **(i)** a escolha de palavras mais simples; **(ii)** a formação de frases e parágrafos curtos; **(iii)** a construção de frases tópicas no início dos parágrafos; **(iv)** a utilização de listas e bullet points; **(v)** o uso moderado de ênfases, como cores contrastantes e negrito; **(vi)** o uso de fontes não serifadas e em tamanho legível; **(vii)** o aproveitamento de espaços em branco; e **(viii)** a introdução de títulos informativos, de preferência, formando questionamentos.

[29]BURKELL, Jacquelyn; MICHETI, Anca; STEEVES, Valerie, Fixing Broken Fences: Strategies for Drafting Privacy Policies Young People Can Understand, **Bulletin of Science, Technology & Society**, n. 2, v. 30, p. 130-143, março, 2010.

3.3. Coleta Excessiva de Dados

Um dos princípios da LGPD refere-se justamente à verificação da real necessidade do uso de determinados dados pessoais, devendo o agente de tratamento se limitar a utilizar o "mínimo necessário" de dados para realização das finalidades de tratamento estabelecidas.[30]

Assim, o agente de tratamento deve verificar se os dados tratados são excessivos ou se são passíveis de serem utilizados de forma a negativamente restringir os direitos da criança ou do adolescente. A avaliação de quais dados são necessários deve ser feita tanto na fase de planejamento de um projeto como de forma periódica nas atividades de tratamento já implementadas. A avaliação de quais dados são realmente necessários deve ser feita caso a caso, tendo sempre como base o melhor interesse da criança ou do adolescente.

Ademais, deve-se destacar que a LGPD proíbe o acesso de crianças a jogos, aplicações de internet ou outras atividades que tenham como contrapartida obrigatória o fornecimento de informações pessoais além das estritamente necessárias à atividade.[31] Este ponto merece especial atenção no caso de aplicativos para celular e/ou serviços web disponibilizados especificamente para serem usados por crianças (ver recomendação abaixo sobre Privacy by Design).

Vale lembrar, contudo, que esse é um princípio que deve ser aplicado a todo e qualquer uso de dados pessoais e não apenas ao tratamento de dados de crianças e adolescentes.

[30] Art. 6º, III da LGPD.

[31] Art. 14, §4º da LGPD.

3.4. Avaliação Inadequada dos Riscos

O tratamento de dados pessoais de crianças e de adolescentes deve ser sempre realizado com base no seu melhor interesse. Assim, qualquer atividade de tratamento deve considerar, seja na fase de planejamento do projeto ou na de implementação, quais são os riscos à privacidade e à proteção dos dados da criança.

A avaliação de risco deve ser realizada, principalmente por meio de:

(i) relatório de impacto à proteção de dados[32],

(ii) utilização de métodos de Privacy by Design[33] e Privacy by Default[34] [35], e

(iii) avaliação do nível de adequação dos fornecedores ou parceiros que venham a ter acesso aos dados. A análise dos riscos deve ser registrada e justificada, para fins de prestação de contas.[36]

Caso a atividade de tratamento de dados venha a ter suas características alteradas (p. ex. utilização de novo fornecedor ou surgimento de uma nova finalidade de uso dos dados), as avaliações de risco devem ser refeitas para se verificar as novas alterações.

[32] Relatório de impacto de proteção de dados é um documento que demonstra como os dados pessoais são coletados e utilizados em uma atividade de tratamento de dados pessoais e quais medidas são adotadas para a mitigação dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares dos dados pessoais.

[33] De forma simples, o conceito de privacy by design refere-se à preocupação em se implementar medidas de proteção à privacidade e aos dados pessoais na fase de desenvolvimento de um produto ou serviço. O conceito foi inicialmente desenvolvido pela ex-diretora da autoridade de proteção de dados de Ontário (Canadá), Ann Cavoukian.

[34] O termo privacy by default é utilizado na legislação da União Europeia, a General Data Protection Regulation 2016/679 (GDPR), e se refere à recomendação de que sistemas de tratamento de dados pessoais sejam configurados por padrão para proteger a privacidade e os dados pessoais de titular, como, por exemplo, ao se configurar por padrão que seja coletado somente o mínimo de dados pessoais.

[35] Ver item 4.8 deste Guia.

[36] Prestação de contas: demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3.5. Comprovação do Consentimento

No caso específico de crianças, a base legal prevista na LGPD para autorizar o tratamento de seus dados pessoais é o consentimento de pelo menos um dos pais ou responsável legal, exceto nas hipóteses em que o tratamento de dados for necessário para proteção da criança ou para contatar os pais ou o responsável legal.[37] Nesse sentido, é dever do agente de tratamento realizar todos os esforços razoáveis para verificar que o consentimento foi realmente dado pelo responsável da criança.[38]

No caso de adolescentes, ou seja, pessoas com idade entre 12 e 18 anos incompletos, a lei não traz essa obrigatoriedade, de modo que os dados poderão ser tratados com fundamento em outras bases legais.

[37]Art. 14 da LGPD.

[38]Art. 14, §5º da LGPD.

Voltar para o índice

4 Como iniciar a adequação da organização à LGPD

Estar em conformidade com a LGPD não precisa ser uma tarefa árdua. Mas, primeiro, é necessário conhecer o perfil do tratamento de dados pessoais de cada organização de acordo com o segmento em que atuam, a fim de se delinear os riscos aos titulares dos dados para que então se empreguem as devidas medidas de mitigação ou de correção das inconformidades.

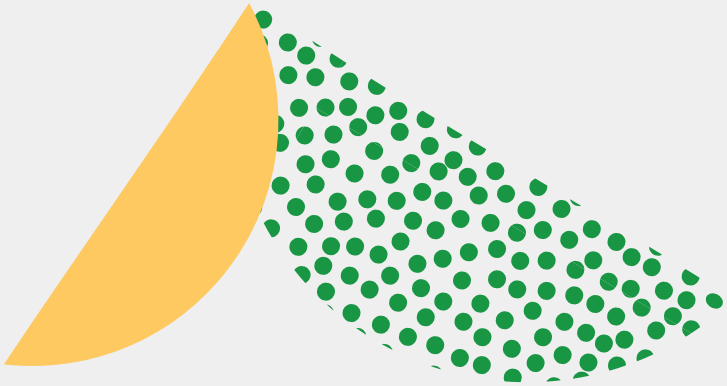
Nesse sentido, após a compreensão de quais são as atividades de tratamento de dados pessoais e os riscos associados, a organização deve estabelecer as prioridades por meio de um plano de trabalho a ser implementado gradualmente, até que se atinja um nível avançado de conformidade com a LGPD. Após a implementação desse primeiro plano de trabalho, deve a organização estabelecer rotinas de adequação que a mantenham em conformidade ao longo do tempo, principalmente em relação à alteração ou à adoção de novas atividades de tratamento.

Abaixo disponibilizamos alguns passos que podem ajudar no início da adequação da sua organização.

4.1. Mapeie as atividades de tratamento

Um passo importante para a conformidade com a LGPD é entender quais dados a organização coleta e o fluxo desses dados em cada uma das áreas/equipes internas. Documentar a maneira como as informações fluem na organização, fazendo um mapeamento de dados pessoais, ajuda a identificar quais atividades de processamento podem causar problemas de conformidade com a LGPD. É nesse mapeamento que a instituição deve atribuir a base legal mais apropriada a cada atividade de processamento, dependendo dos dados pessoais envolvidos e a finalidade de processamento.

Segue abaixo um modelo de mapeamento que pode servir como um bom ponto de partida:



Mapeamento de Dados Pessoais

Dados Pessoais	Fonte: como e de onde os dados foram obtidos?	Finalidade de uso dos dados	Armazenamento: indicar onde os dados são armazenados e quem tem acesso	Transferência: indicar se os dados são transferidos a terceiros	Base Legal	São tratados dados sensíveis?	São tratados dados de crianças?
Nome CPF Endereço E-mail	Formulário de Cadastro do Website	Cadastro	Google Cloud	Não há	Consentimento	Não	Não
[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]

4.2. Ajuste seu website

Realizar ajustes nos websites são essenciais para a conformidade. Na prática, esse será o primeiro lugar em que as pessoas procurarão informações para verificar a conformidade ou não de uma organização.

A **Políticas de Privacidade:** a política de privacidade da organização tem o objetivo de explicar os dados pessoais tratados, assim como as finalidades de tratamento de tais dados em relação ao público externo, devendo ser disponibilizada de forma acessível no website e conter:

(i) as finalidades de tratamento dos dados em relação ao público externo (doadores, parceiros etc.);

(ii) a identificação do "Controlador"[39] dos dados pessoais, bem como suas informações de contato;

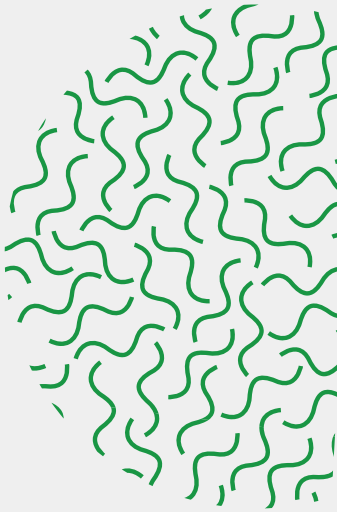
(iii) informações sobre eventual uso compartilhado de dados; e

(iv) menção explícita aos direitos dos titulares e o procedimento para exercê-los.

[39]A LGPD define o termo "controlador" como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5, VI, da LGPD). As obrigações da LGPD se aplicam majoritariamente aos "controladores".

B **Formulários de Cadastro:** eventuais formulários de cadastro deverão ser devidamente ajustados, especialmente para que sejam coletados apenas os dados necessários, e para que os propósitos da coleta sejam explicados aos titulares.

C **Coleta de Cookies:** Caso o website da organização utilize cookies ou outras tecnologias de coleta de dados pessoais dos usuários, recomenda-se a criação de um *cookie notice* – ou seja, um aviso ou informativo em seu website sobre quais cookies podem ser coletados do usuário, devendo o aviso aparecer durante a navegação do usuário (p. ex. na página inicial).



4.3. Permita que os titulares exerçam seus direitos

De acordo com a LGPD, os titulares dos dados têm vários direitos[40], que a organização, como agente de tratamento dos dados (seja Controladora ou Operadora[41]), deve garantir. Dentre eles, destacam-se:

Direito de acesso: significa que o titular tem o direito de receber da organização as informações sobre o tratamento de seus dados. Isso pode ser feito, por exemplo, por meio da disponibilização de uma cópia dos dados pessoais que a organização detenha, e/ou por meio da disponibilização de uma política de privacidade;

Direito de retificação: significa que o titular tem o direito de solicitar a correção e/ou retificação dos seus dados pessoais, caso identifique incorreções;

[40]Ver arts. 18 e 20 da LGPD.

[41]A LGPD define o termo "operador" como a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5, VII, da LGPD).

Direito de exclusão, quando possível: significa que o titular pode solicitar a exclusão dos seus dados pessoais dos sistemas e bases de dados da organização. Quando ocorre esse tipo de solicitação, os dados coletados devem ser excluídos, salvo se houver uma razão para mantê-los, como uma obrigação legal ou necessidade de preservar estes dados para resguardo de direitos da organização; e

Direito de explicação sobre uma decisão automatizada: o titular tem direito de entender os motivos que levaram a ser submetido a uma decisão automatizada e qual a lógica decisória utilizada, resguardados os segredos industriais e comerciais. Por exemplo, uma explicação sobre direcionamento de publicidade *on-line*.

A implementação de todos esses direitos de uma maneira totalmente automatizada pode ser uma tarefa árdua e bastante custosa, especialmente para organizações do terceiro setor. É importante ressaltar que a LGPD não exige que o exercício desses direitos seja totalmente automatizado, mas exige que a resposta ao titular seja feita de maneira imediata, quando em formato simplificado, ou em até **15 dias** contados da data do requerimento do titular, quando tiver que ser feita de forma completa (ou seja, a resposta indicar a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento).

Portanto, é recomendável que inicialmente seja criado apenas um **canal de contato**, específico para atendimento de questões sobre privacidade e proteção de dados, por meio do qual o titular poderá exercer seus direitos. Posteriormente, dependendo da frequência e dos tipos de solicitações, a organização poderá refletir sobre a utilização de ferramentas automatizadas, total ou parcialmente, de forma a responder aos direitos dos titulares.

4.4. Realize treinamentos

A realização de treinamentos, ações educativas e de conscientização dos empregados, funcionários, colaboradores e voluntários serve para reforçar as políticas e práticas de privacidade e proteção de dados da organização e são essenciais para transmitir os parâmetros a serem implementados.

Os treinamentos devem ser realizados especialmente nas organizações em que os empregados, funcionários, colaboradores ou voluntários tenham contato com usuários, clientes ou doadores, pois, por meio desses contatos, é possível que sejam coletados diversos dados pessoais de maneira excessiva ou que o titular questione sobre o uso de seus dados e sobre seus direitos.

Dependendo do tamanho da instituição, tais ações podem incluir métodos um pouco mais informais, tais como:

/ treinamentos em sala de aula;

/ campanhas e posters; aprendizagem online por meio de streaming, vídeos e sites; e

/ workshops.

Além dos treinamentos, também é recomendado que a organização documente, por meio de políticas, a forma como os dados devem ser tratados, armazenados e disponibilizados por todas as áreas da organização, para orientar e estabelecer as diretrizes corporativas para a proteção das informações e alocação de responsabilidades.

4.5. Avalie seus fornecedores e parceiros

Para estar em conformidade com a LGPD, a organização precisa verificar o nível de adequação dos seus fornecedores e parceiros. Para realização dessa análise, primeiro é necessário avaliar se o fornecedor/parceiro se qualifica como **(i)** Controlador, **(ii)** Operador ou **(iii)** Controlador conjunto[42] em relação à organização. Os tipos de agentes de tratamento definidos na LGPD apresentam responsabilidades distintas, sendo que o Controlador é o principal responsável pelos dados, tendo maior número de obrigações legais quando comparado à figura do Operador. Tais responsabilidades poderão envolver, por exemplo, a atribuição de bases legais que justificam o uso dos dados, a obrigação pelo atendimento dos direitos dos titulares, a elaboração de relatórios de impacto, entre outras.

Após a definição do papel dos agentes de tratamento e de como os dados pessoais serão usados, é importante a elaboração de um contrato. Contudo, quando se trata de organizações do terceiro setor, a elaboração e revisão de contratos, bem como a imposição de cláusulas e disposições contratuais, embora desejável, nem sempre é possível. Isso pode requerer um investimento de tempo e dinheiro, além de exigir um poder de barganha, que nem sempre estão disponíveis às organizações do terceiro setor.

[42]Para maiores detalhes, ver o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado" elaborado pela ANPD. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>

Sendo assim, caso não seja possível negociar e/ou revisar os contratos firmados com os fornecedores e parceiros, sugere-se que as instituições do terceiro setor, ao menos, se atentem aos seguintes pontos:

Verifique a política de privacidade de seus parceiros e fornecedores. Basicamente, para que a política esteja minimamente adequada à LGPD, tenha certeza de que ela menciona os seguintes pontos:

/ o nome da organização (incluindo CNPJ) e o nome do responsável pelas questões relacionadas à privacidade e proteção de dados;

/ o que a organização faz com esses dados e a razão que justifica o seu uso (finalidades e bases legais, respectivamente);

/ com quem e como os dados são compartilhados, incluindo qualquer compartilhamento internacional de dados;

/ por quanto tempo os dados são armazenados; e

/ como o titular pode exercer seus direitos.

Verifique as medidas e certificações de segurança da informação que são utilizadas por seus parceiros e fornecedores. Certificações como ISO 27001, ISO 27701, ISO 27002, e certificados específicos para segurança em cloud/computação em nuvem podem demonstrar um nível avançado de conformidade com a LGPD.

Verifique se o parceiro ou fornecedor já foi multado ou sofreu forte investigação ainda não resolvida. Imposições de multas e práticas de investigação pelo Ministério Público ou pela ANPD podem significar um alerta para a negociação com esse parceiro ou fornecedor.

/ Entes públicos

No caso de parcerias com entes públicos, a utilização de um instrumento contratual específico é fortemente recomendada para justificar o compartilhamento de dados pessoais com uma organização do terceiro setor. Isso porque são restritivas as hipóteses da LGPD que autorizam o poder público a transferir dados pessoais a entidades privadas, sendo elas:

(i) previsão normativa/regulatória ou

(ii) contratual.[43]

Em relação aos fins para os quais os dados serão usados, pode haver menor margem para negociação dessas finalidades, pois o tratamento pelo Poder Público deve seguir a persecução do interesse público (por exemplo, uso dos dados para execução de políticas públicas respaldadas na legislação ou normas administrativas).

Ainda, a depender de como os dados serão utilizados, é necessário avaliar o enquadramento da organização como agente de tratamento de dados - se Controladora, Operadora, ou Controladora conjunta com o Poder Público – para entender os limites e responsabilidades no tratamento dos dados pessoais.

[43]LGPD: "Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: [...] IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres.

4.6. Utilize técnicas de anonimização e pseudonimização

/ Anonimização

O que é? A anonimização ocorre quando os dados pessoais de um titular não podem mais ser ligados a ele, ou seja, é a transformação de um dado pessoal em um dado que não pode ser vinculado ao seu titular. A vantagem é que a LGPD não se aplica para dados efetivamente anonimizados.

Como anonimizar? Para garantir a anonimização dos dados pessoais, a organização pode se utilizar das seguintes técnicas:

1. **Supressão de dados:** Uma das técnicas de anonimização mais efetivas. Nela, os valores e informações são substituídos por caracteres especiais e nulos que fazem com que os dados pessoais não identifiquem mais o titular dos dados, de modo que os dados acabam se tornando dados anonimizados. Nesse caso, um CPF de n° 123.456.789-00 passa a ser: yyzz, por exemplo.[44]

[44] ICO (Information Comissioner's Office): Anonimização: código de prática de gestão de risco de proteção de dados. Novembro, 2012. "A supressão local consiste em substituir o valor observado de uma ou mais variáveis em um determinado registro com um valor 'nulo'. Isso é particularmente adequado para variáveis-chave categóricas (uma variável-chave é uma variável na qual um pesquisador está particularmente interessado). Quando combinações de tais variáveis são problemáticas, a supressão local consiste em substituir um valor observado por um valor 'nulo' ou algum outro que mostre que o valor original foi suprimido. O objetivo do método é reduzir o conteúdo de informações de combinações raras. O resultado é um aumento na contagem de frequência de registros contendo a combinação modificada" (em tradução livre). A versão original, em inglês, está disponível em: Disponível em: < https://ico.org.uk/media/1061/anonymisation-code.pdf> . Acesso em: 26/08/2021.

2 **Generalização:** Nessa técnica de anonimização, dados específicos são substituídos por dados bem mais genéricos, para, assim, o titular dos dados passar a se tornar alguém não identificável. Podemos citar como exemplo o caso em que ao invés de armazenar o endereço de um titular de dados, armazena-se a região em que ele reside. Assim, o titular dos dados não pode ser identificado.[45]

3 **Perturbação (adição de ruído):** A técnica que consiste em substituir as informações relacionadas aos dados dos titulares por outras informações aleatórias e inventadas. Assim, consequentemente, os dados não poderão mais identificar ou tornar identificável o titular, de modo que poderão ser considerados dados anonimizados.[46]

[45] Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995. Parecer 05/2014 sobre Técnicas de Anonimização. Abril, 2014. "A generalização é a segunda família de técnicas de anonimização.Essa abordagem consiste em generalizar ou diluir os atributos dos titulares dos dados, modificando a respectiva escala ou ordem de magnitude (ou seja, uma região em vez de uma cidade, um mês em vez de uma semana). Enquantoa generalização pode ser eficaz para evitar a identificação, não permite a anonimização eficaz em todos os casos; em particular, requer abordagens quantitativas específicas e sofisticadas para evitar a vinculação einferência." (tradução livre). Versão original, em inglês, disponível em: Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> . Acesso em: 26/08/2021> . Acesso em: 26/08/2021.

[46]ICO: Information Comissioner's Office. Anonimização: código de prática de gestão de risco de proteção de dados. Novembro, 2012. "Adição de ruído, método aplicado a dados numéricos, consiste em adicionar um valor aleatório ε a todos os valores na variável a ser protegida. A distribuição de ε tem média zero e variância pré-definida σ2" (tradução livre) Versão original, em inglês, disponível em: < https://ico.org.uk/media/1061/anonymisation-code.pdf>. Acesso em: 26/08/2021.

Atenção!

Existem diferentes graus possíveis de anonimização. A LGPD considera a anonimização de forma relativa, devendo o agente de tratamento levar em consideração para a avaliação da qualidade da anonimização (art. 46, § 1º):

(a) o estado atual da tecnologia, e

(b) quais seriam as chances de se reverter a anonimização considerando os custos e a viabilidade técnica.

Assim, a depender dos riscos relativos à possibilidade de reversão da anonimização, pode ser necessário a utilização de técnicas mais robustas de anonimização, para que os dados sejam considerados anonimizados perante a LGPD.

/ Pseudonimização

O que é? A pseudonimização é na verdade uma medida de segurança da informação que não se confunde com a anonimização. Na técnica de pseudominização, os dados pessoais são codificados assim, somente quem possui a chave de descodificação pode novamente associar os dados ao titular.[47]

Como pseudonimizar? É possível, por exemplo, substituir os nomes de uma lista por determinado código (João por 12X1), sendo que a tabela de correspondência será mantida em arquivo separado. Assim, somente quem tem acesso à tabela de correspondência conseguirá identificar quem são os titulares. A utilização de técnicas de criptografia é uma forma de pseudonimizar dados pessoais.

Dessa forma, verifica-se que a pseudonimização, como o nome já indica, apenas impede a identificação direta do titular, sendo, portanto, uma medida de segurança da informação. Porém, a associação do dado ao seu titular será possível a partir das informações adicionais de correspondências mantidas em separado.[48] Esse tipo de técnica pode ser útil para controlar o acesso interno a determinadas informações ou impedir que esses dados possam ser usados por terceiros em caso de incidente de segurança (p. ex. um vazamento de dados pseudonimizados).

[47]Nesse sentido, o art. 13, §4º da Lei Geral de Proteção de Dados, determina: "a pseudonimização é o tratamento 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".

[48]Infra News Telecom. Anonimização, pseudonimização e criptografia: Perguntas frequentes, definições e o que diz a LGPD. "Ela representa somente um meio mais seguro de tratar os dados pessoais quando ainda há um interesse em manter os identificadores diretos do titular. A ideia é que estes sejam mantidos de forma separada". Disponível em: <https://www.infranewstelecom.com.br/anonimizacao-pseudonimizacao-e-criptografia-perguntas-frequentes-definicoes-e-o-que-diz-a-lgpd/> . Acesso em: 18/08/2021.

4.7. Relate incidentes de segurança

Outra obrigação muito importante trazida pela LGPD é a de o Controlador relatar incidentes de segurança da informação que possam acarretar risco ou dano relevante aos titulares. Um incidente de segurança significa não só um vazamento de dados, mas todo e qualquer acesso, alteração ou indisponibilização de dados de forma indevida: ou qualquer outro tratamento indevido de dados pessoais.

Se houver um incidente envolvendo dados pessoais, a LGPD exige que tal incidente seja comunicado aos titulares afetados e à Autoridade Nacional de Proteção de Dados. A comunicação deverá ser feita em prazo razoável[49] e deverá mencionar:

natureza dos dados pessoais afetados	os riscos relacionados ao incidente
informações claras sobre os titulares envolvidos	os motivos da demora, no caso de a comunicação não ter sido imediata
a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados	as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo

[49] Vale ressaltar que atualmente a recomendação da Autoridade Nacional de Proteção de Dados é que tal comunicação seja feita no prazo de 48 horas.

4.8. Conduza análises privacy by design & privacy by default

O conceito de Privacy by Design foi inicialmente desenvolvido por Ann Cavoukian, ex-diretora da autoridade de proteção de dados de Ontário (Canadá), e refere-se à preocupação em implementar medidas de proteção à privacidade e aos dados pessoais desde a fase de desenvolvimento e concepção de um produto ou serviço.[50]

O termo Privacy by Default, de maneira similar, é utilizado na legislação europeia e remete à recomendação de que sistemas de tratamento de dados pessoais sejam configurados, por padrão, para proteger a privacidade e os dados pessoais do titular – é o caso, por exemplo, de determinado software configurado por padrão para que seja coletado apenas o mínimo de dados necessários à sua operação, tendo o usuário que autorizar qualquer coleta adicional.

Tais abordagens apontam para a necessidade de se levar em conta a privacidade do indivíduo durante todo o processo de desenvolvimento de produtos ou serviços. Uma análise Privacy by Design (PbD) pode ser conduzida por meio da aplicação dos sete princípios estabelecidos por Ann Cavoukian. [51] [52]

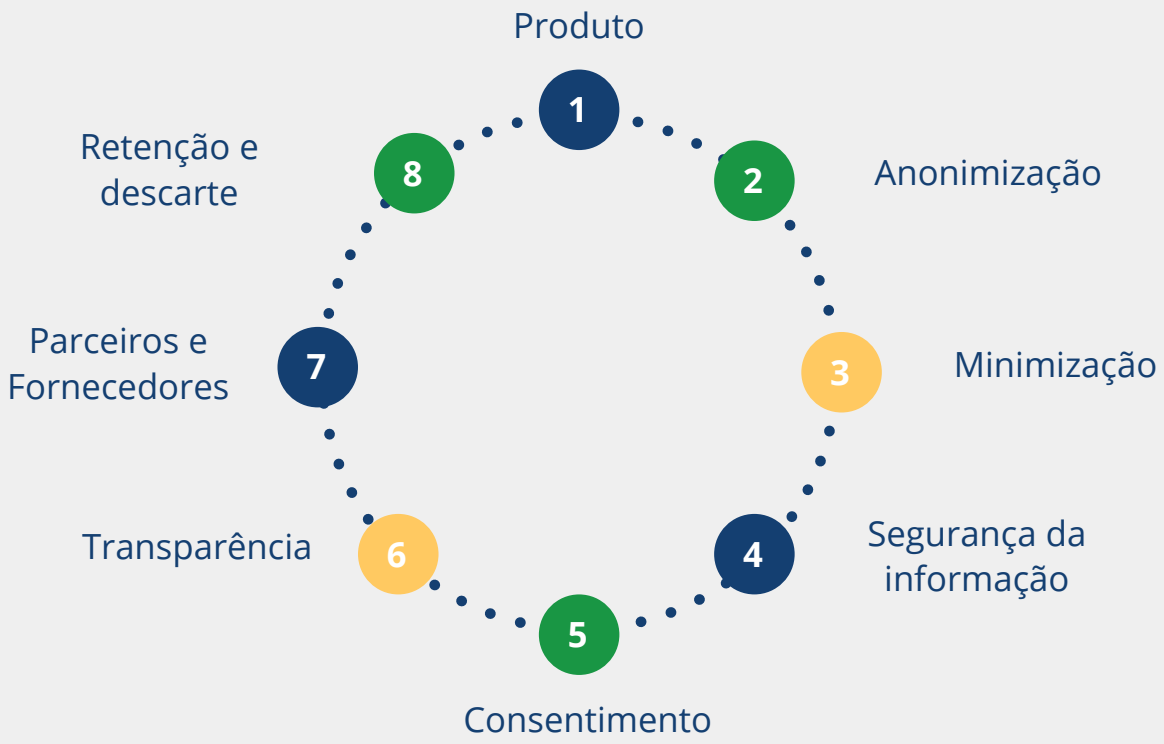
[50]Note-se que o conceito de privacy by design foi devidamente incorporado pela LGPD: "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. [...] § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".

[51]CAVOUKIAN, Ann. Privacy by Design - 7 Foundational Principles. 2009. Disponível em:<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.

[52]Existem também outras metodologias para aplicação de privacy by design. Por exemplo: European Union Agency for Network and Information Security (ENISA). Privacy and Data Protection by Design – from policy to engineering. 2014. Disponível em: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

Para facilitar essa análise, o Baptista Luz Advogados desenvolveu um Roadmap de PbD (imagem a seguir), que ajudará os desenvolvedores de produtos e serviços a pensar na privacidade e proteção de dados desde o início. Para entender melhor cada etapa do Roadmap, confira o fluxograma do Anexo II.

Roadmap de *Privacy by Design*



O Instituto Ayrton Senna, por exemplo, no contexto do aplicativo **Motivação+** – iniciativa educacional voltada para jovens de 14 a 21 anos que tem como objetivo auxiliar o desenvolvimento socioemocional e a construção dos projetos de vida desses jovens, tanto pessoais quanto coletivos –, entendeu necessária a elaboração de análises de risco de proteção de dados e de avaliações da jornada do usuário pelas plataformas digitais. Ao aplicar os princípios de Privacy by Design e Privacy by Default nas atividades de tratamento de dados pessoais dos aplicativo Motivação+, foi possível identificar meios para conciliar a missão do projeto com o melhor interesse da criança em ter a sua privacidade preservada – o que resultou na adoção de mecanismos para melhor transparência com o usuário, implementação de travas tecnológicas para limitar o acesso à plataforma de pessoas que não se enquadram na faixa etária proposta, revisão dos termos de uso, entre outros

4.9. Regras para agentes de tratamento de pequeno porte

É possível que organizações do terceiro setor enquadrem-se na definição de agentes de pequeno porte.[53] Nesses casos, as organizações podem beneficiar-se de um tratamento jurídico diferenciado, desde que não realizem tratamento de alto risco para os titulares (p. ex. tratamento em larga escala de dados sensíveis ou dados de crianças, adolescentes ou idosos).[54] [55]

Dentre as obrigações dispensadas ou flexibilizadas pela ANPD para agentes de tratamento de pequeno porte estão:

(i) A elaboração e manutenção de registro de operações de tratamento de dados pessoais de forma simplificada, cujo modelo será disponibilizado pela ANPD tempestivamente;[56]

(ii) A simplificação/flexibilização do procedimento de comunicação de incidente de segurança por parte das organizações;[57]

[53] Resolução CD/ANPD nº 2/2022: "Art. 2º Para efeitos deste regulamento são adotadas as seguintes definições: I - agentes 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 [...]."

[54] Art. 3º, I da Resolução CD/ANPD nº 2/2022.

[55] Art. 4º da Resolução CD/ANPD nº 2/2022.

[56] Art. 9º da Resolução CD/ANPD nº 2/2022.

[57] Art. 10º da Resolução CD/ANPD nº 2/2022.

(iii) A não-obrigatoriedade da indicação de um encarregado de proteção de dados, o que não desobriga a organização de disponibilizar um canal de comunicação com o titular de dados;[58]

(iv) A possibilidade da elaboração de uma política de segurança da informação simplificada que contemple apenas os requisitos essenciais e necessários para o tratamento de dados pessoais;[59]

(v) A concessão de prazo em dobro para (a) o atendimento às solicitações dos titulares; (b) a comunicação referente a incidentes de segurança, salvo em caso de potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional; (c) o fornecimento de declaração clara e completa ao titular; e (d) a apresentação de informações solicitadas pela ANPD a outros agentes de tratamento;[60] e

(vi) A possibilidade de fornecimento da declaração simplificada no prazo de 15 dias, contados da data do requerimento do titular.[61]

Assim, cabe às organizações analisarem individualmente se as suas atividades se enquadram nas definições estabelecidas pela ANPD no Regulamento nº 2/2022.

[58] Art. 11º da Resolução CD/ANPD nº 2/2022.

[59] Art. 13º da Resolução CD/ANPD nº 2/2022.

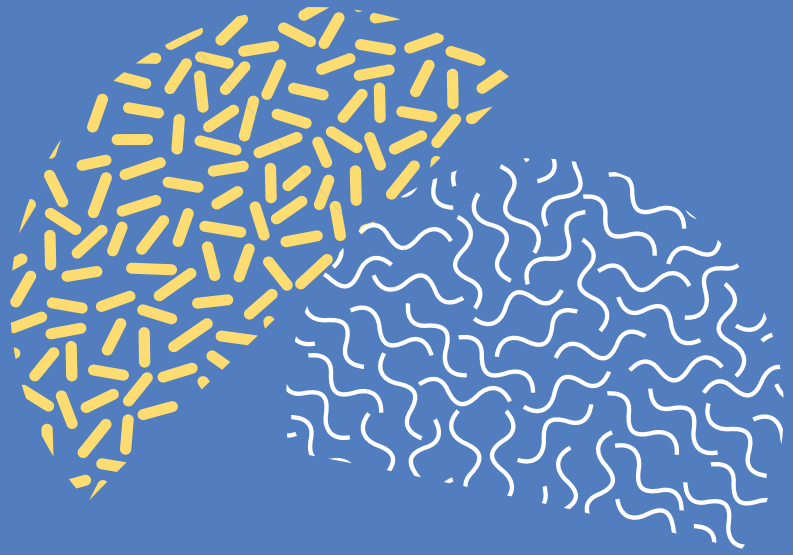
[60] Art. 14º da Resolução CD/ANPD nº 2/2022.

[61] Art. 15º da Resolução CD/ANPD nº 2/2022.

Voltar para o índice

5 Exemplos de Produtos e Serviços oferecidos pelo Terceiro Setor

O objetivo deste tópico é, com base nos comentários e recomendações feitas ao longo do guia, citar exemplos de situações comuns nas quais organizações do terceiro setor realizam o tratamento de dados pessoais, de acordo com os serviços e produtos que oferecem.



5.1. Organização não governamental que fornece serviços de saúde

A LGPD determina que informações de saúde – como informações genéticas, biométricas e relacionadas à vida sexual – são **dados pessoais sensíveis**.[61] Dados pessoais cuja inferência pode levar a dados sensíveis também devem ser, por equiparação, considerados como tais. Os dados pessoais sensíveis devem estar sujeitos a medidas adicionais de proteção, uma vez que têm um potencial de gerar restrições significativas ao exercício de direitos fundamentais pelo titular dos dados.[62]

Por exemplo, a Agência Nacional de Saúde (ANS) já reforçou preocupações a respeito do uso de dados sensíveis referentes à sexualidade de pacientes – por meio de inferências –, ao estado de saúde de empregados no contexto de recursos humanos, e à identificação de doenças estigmatizantes.[63] Quanto às doenças estigmatizantes, em especial, a Lei n. 14.289/2022 recentemente impôs uma necessidade de preservação do sigilo quanto à condição da pessoa acometida. [64]

[61]Art. 5º, II, da LGPD.

[62]Autoridade Nacional de Proteção de Dados; Tribunal Superior Eleitoral. Guia orientativo: aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral. Brasília: Tribunal Superior Eleitoral, 2021, p. 10.

[63]ANS. Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES, item 4.3. Disponível em https://bit.ly/374qvO8. Acesso em 17.01.2022.

[64]"Art. 1º Esta Lei dispõe sobre a obrigatoriedade de preservação do sigilo sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose, nos casos que estabelece."

Diante desse cenário, as organizações devem observar, entre outros, os seguintes fatores ao tratarem dados pessoais de saúde:

- avaliar a necessidade de obtenção de **consentimento específico e destacado** de pacientes, tendo em vista as exigências regulatórias e da LGPD;
- preservar a **confidencialidade das informações de saúde** coletadas, principalmente entre colaboradores da organização e terceiros com acesso autorizado;
- aplicar **medidas adicionais de segurança da informação** no armazenamento e acesso às informações de saúde, tanto em meio físico quanto digital; e
- avaliar **possíveis inferências** de dados pessoais sensíveis a partir de dados pessoais ou outras informações, considerando o contexto específico de tratamento das informações.

5.2. Instituto comprometido com serviços educacionais a crianças e adolescentes

Como já mencionado, o tratamento de dados de crianças e adolescentes requer medidas mais protetivas por parte da organização responsável pelas informações.

A LGPD determina que "o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal" [65]. Com isso, além de impor ao controlador dos dados a **obrigação de obter o consentimento parental para crianças**, a lei condiciona esse consentimento a um nível maior de proteção, devendo ser obtido de forma específica e destacada. As únicas exceções de dispensa de consentimento previstas na lei seriam **(i)** para contatar o pai ou responsável legal da criança, uma única vez e sem armazenamento dos dados; e **(ii)** para proteção da criança, vedado o compartilhamento dos dados em ambos os casos sem o consentimento.[66]

O tratamento de dados também deve sempre observar o melhor **interesse da criança**,[67] como previsto na Convenção sobre Direitos da Criança.[68] Trata-se de um princípio complexo, flexível e adaptável, analisado caso a caso, que assegura o pleno e efetivo gozo de todos os outros direitos reconhecidos na Convenção e o desenvolvimento da criança em sentido holístico. Os melhores interesses devem ser analisados no contexto em que cada criança está inserida e considerando seu estágio de maturidade.[69]

[65]Art. 14, § 1º, da LGPD.

[66]Art. 14, § 3º, da LGPD.

[67]Art. 14, caput, da LGPD.

[68]A Convenção considera criança "todo ser humano com menos de 18 anos de idade", de maneira diversa da legislação brasileira que, em termos técnicos, diferencia a criança do adolescente. O ECA define como criança pessoa com até doze anos incompletos (art. 2º).

[69]Comitê sobre os Direitos da Criança das Nações Unidas. **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration** (art. 3, para. 1), p. 04.

Assim, ao tratarem dados pessoais de crianças e adolescentes, as organizações devem observar os fatores referentes:

- à avaliação da **necessidade de obtenção do consentimento** parental dos pais ou responsáveis legais pela criança;
- em plataformas digitais, à aplicação de **mecanismos de controle parental** (verificação de idade - *age gate*) aos conteúdos direcionais especificamente a crianças e adolescentes;
- ao **meio de obtenção do consentimento** parental, incluindo, por exemplo, transações financeiras ou envio de e-mail de confirmação aos pais e responsáveis; e
- ao provimento de **mecanismos de transparência** adaptados às necessidades e capacidades evolutivas da criança e/ou do adolescente.

5.3. Entidade beneficente que atua no acolhimento e apoio a pessoas idosas

A LGPD contém regra específica para os dados pessoais de pessoas idosas (idade igual ou superior a 60 anos), determinando que o tratamento de informações dessa categoria de titulares seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento.[70] Dessa forma, no contexto das atividades da entidade beneficente, a LGPD deve ser interpretada em conjunto com os artigos 48 a 51 do Estatuto do Idoso (Lei n. 10.741/2003) e os demais fundamentos da lei.

Nesse sentido, importante notar que o Estatuto do Idoso exige o armazenamento de certas informações sobre a pessoa idosa,[71] incluindo **(i)** a data e circunstância do atendimento, **(ii)** o nome do idoso, de seus responsáveis e parentes, **(iii)** endereços e cidades de habitação, **(iv)** a relação de seus pertences, **(v)** o valor de contribuições e **(vi)** demais dados que possibilitem a identificação e individualização do atendimento.

O tratamento dessas informações, no entanto, deve estar em linha com a "preservação da identidade do idoso e oferecimento de respeito e dignidade"[72]. Diante disso, alguns cuidados devem ser observados, incluindo:

[70]Art. 55-J, XIX, da LGPD.

[71]Art. 50, XV, do Estatuto do Idoso.

[72]Art. 49, VI, do Estatuto do Idoso.

- disponibilização de **suporte físico** a informações e documentos que são apenas fornecidos digitalmente;
- adaptação dos mecanismos de transparência às necessidades do idoso, satisfazendo **requisitos de acessibilidade**;
- reavaliação dos usos e compartilhamentos de dados à luz do **princípio da não-discriminação,** sobretudo os relacionados à previdência e assistência social;
- celebração de **acordos de confidencialidade** com as pessoas envolvidas, visando à preservação da identidade do idoso; e
- armazenamento **seguro** e **sigiloso** do histórico de atendimento do idoso, que pode constituir perfil revelando informações previdenciárias, financeiras e de saúde.

Voltar para o índice

6 Conclusão

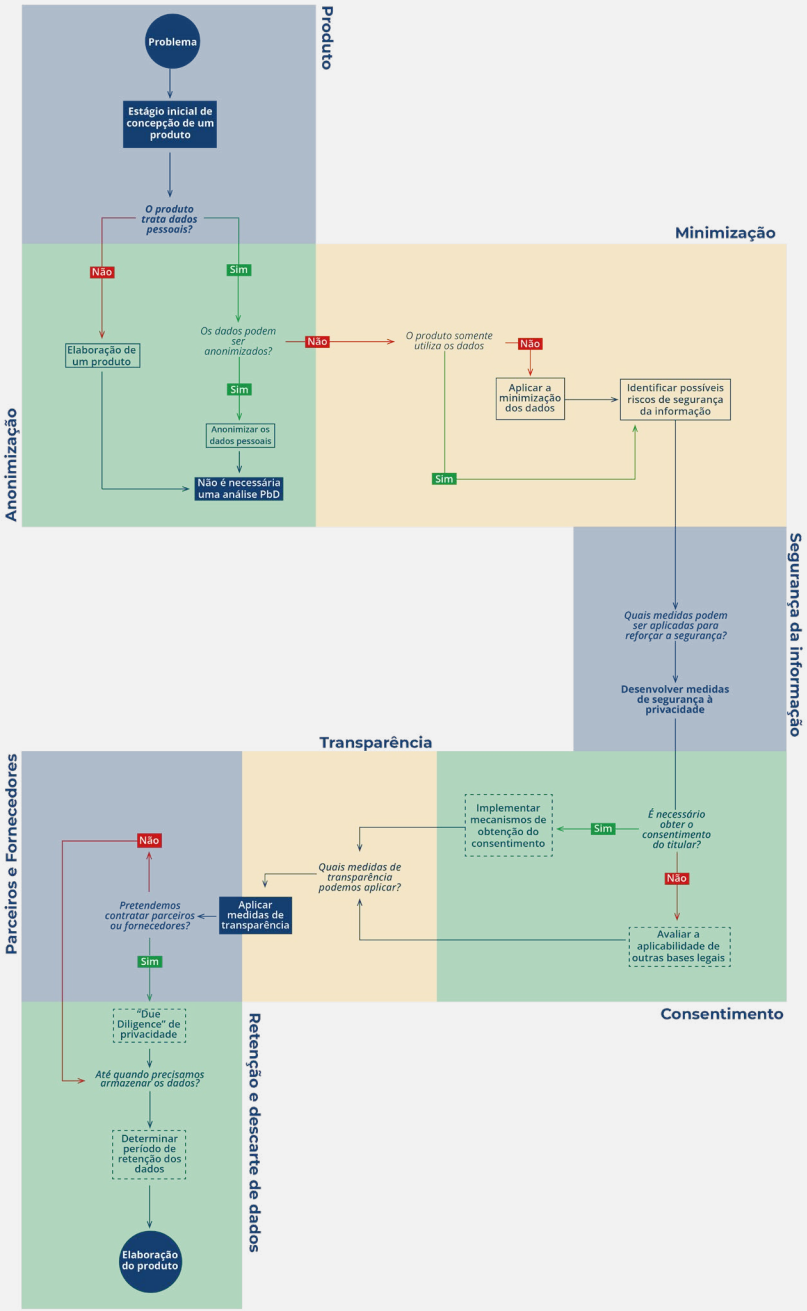
As organizações do terceiro setor enfrentam desafios próprios às atividades de tratamento de dados que realizam. Embora se enquadrem como entidades sem fins lucrativos e que visam fins sociais, elas se sujeitam à LGPD da mesma forma que o setor privado com fins lucrativos. Assim, as organizações devem mapear suas atividades de tratamento e observar as normas setoriais sobre privacidade e proteção de dados pessoais que lhes sejam aplicáveis.[73]

Há a necessidade, portanto, de se conhecer o perfil do tratamento de dados de cada organização de acordo com o segmento em que atuam, a fim de se delinear os riscos inerentes às atividades e aos titulares dos dados, para que então empreguem as devidas medidas de mitigação ou de correção das inconformidades. O respeito à privacidade e aos dados pessoais é também um compromisso social que deve permear a missão institucional do terceiro setor como vanguarda da sociedade.

[73]Recomendamos também a consulta ao site da ANPD (https://www.gov.br/anpd/pt-br), que disponibiliza materiais como guias orientativos sobre diferentes temas da LGPD.

Voltar para o índice

Anexo I – Fluxograma de Aplicação do Privacy by Design


Produto
Problema
Estágio inicial de concepção de um produto
O produto trata dados pessoais?
Não
Sim
Elaboração de um produto
Os dados podem ser anonimizados?
Não
Sim
Anonimizar os dados pessoais
Não é necessária uma análise PbD
Anonimização
Minimização
O produto somente utiliza os dados
Não
Aplicar a minimização dos dados
Identificar possíveis riscos de segurança da informação
Sim
Segurança da informação
Quais medidas podem ser aplicadas para reforçar a segurança?
Desenvolver medidas de segurança à privacidade
Transparência
Parceiros e Fornecedores
Não
Pretendemos contratar parceiros ou fornecedores?
Aplicar medidas de transparência
Quais medidas de transparência podemos aplicar?
Implementar mecanismos de obtenção do consentimento
Sim
É necessário obter o consentimento do titular?
Não
Avaliar a aplicabilidade de outras bases legais
Consentimento
Sim
"Due Diligence" de privacidade
Até quando precisamos armazenar os dados?
Determinar período de retenção dos dados
Elaboração do produto
Retenção e descarte de dados

Voltar para o índice

Anexo II - Fontes para aprofundamento

Neste tópico listamos publicações, guias e demais materiais que podem auxiliar as entidades do terceiro setor a implementar melhores práticas de proteção da privacidade e de dados pessoais.

1. Instituições de Referência

/ Instituto de Tecnologia e Sociedade – ITS Rio

Link: https://itsrio.org

/ Safernet

Link: https://new.safernet.org.br

2. Uso de Dados de Crianças

i. Relatório de Boas Práticas: Proteção de Dados de Crianças e Adolescentes

Elaborado por: Instituto de Tecnologia e Sociedade – ITS Rio

Link: https://itsrio.org/pt/publicacoes/relatorio-de-boas-praticas-protecao-de-dados-de-criancas-e-adolescentes/

ii. Age appropriate design: a code of practice for online services

Elaborado por: Information Commissioners's Office - ICO

Link: https://ico.org.uk/for-organisations/childrens-code-hub/

iii. Age appropriate design: a code of practice for online services

Elaborado por: The Data Protection Commission - DPC

Link: https://www.dataprotection.ie/en/dpc-guidance/blogs/the-children-fundamentals

3. Avaliação de Risco à Proteção de Dados Pessoais

iv. Gestión del Riesgo y Evaluácion de Impacto en Tratamientos de Datos Personales

Elaborado por: Agencia Española de Protección de Datos

Link: https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

4. Anonimização de Dados Pessoais

v. Opinion 05/2014 on Anonymisation Techniques

Elaborado por: Article 29 Data Protection Working Party

Link: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

vi. A Visual Guide to Practical Data De-Identification

Elaborado por: Future of Privacy Forum

Link: https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification/

vii. Student Data and De-Identification: Understanding De-Identification of Education Records and Related Requirements of FERPA

Elaborado por: Future of Privacy Forum

Link: https://fpf.org/blog/student-data-and-de-identification/

viii. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

Elaborado por: United States Department of Health and Human Services

Link: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

ix. 10 Malentendidos Relacionados con la Anonimización

Elaborado por: Agencia Española de Protección de Datos

Link: https://www.aepd.es/es/documento/10-malentendidos-anonimizacion.pdf

b/luz

Para saber mais, acesse nosso site ou nos acompanhe nas redes sociais.

baptistaluz.com.br