MANUAL PRÁTICO DE ADEQUAÇÃO À

Lei Geral de Proteção de Dados para Organizações da Sociedade Civil

idec
Instituto Brasileiro de Defesa do Consumidor

2021

MANUAL PRÁTICO DE ADEQUAÇÃO À

Lei Geral de Proteção de Dados para Organizações da Sociedade Civil

idec
Instituto Brasileiro de Defesa do Consumidor

2021

O QUE VOCÊ VAI ENCONTRAR NESTE MANUAL

3. CONHECENDO MELHOR A LGPD

Erguendo as paredes: Bases legais para o tratamento de dados

Cobrindo sua casa: Direitos dos/as titulares de dados

4. ADEQUAÇÃO NA PRÁTICA – PASSO A PASSO

APRESENTAÇÃO

É com grande satisfação que nós, do Instituto Brasileiro de Defesa do Consumidor (Idec), desenvolvemos e compartilhamos com você este Manual. Um material com tudo o que Organizações da Sociedade Civil (OSCs) precisam saber e fazer para se adequarem à Lei Geral de Proteção de Dados (LGPD), que regulamenta o armazenamento e a utilização de dados pessoais.

Com a missão de promover relações de consumo mais justas, o Idec participou ativamente da construção dessa legislação, que é fundamental para estabelecer e garantir direitos a todas as pessoas que fornecem dados pessoais para acessar produtos ou serviços. Também assumimos um importante papel de educar titulares de dados para que conheçam seus direitos relacionados à privacidade e proteção de dados e os exerçam perante instituições que coletam e armazenam esse tipo de informação.

Como a melhor forma de ensinar é dar o exemplo, desde 2019, temos revisto nossas práticas para garantir a proteção dos dados das pessoas que se relacionam com o Idec. A partir dessa experiência, que nos agregou uma perspectiva prática sobre o tema, elaboramos este Manual para apoiar outras OSCs em seus processos de adequação à LGPD.

Ao longo das próximas páginas, vamos desconstruir algumas *fake news* que podem fazer a LGPD parecer um bicho de sete cabeças ou uma ameaça para sua organização; vamos percorrer a Lei, apresentando seus princípios, bases legais e os direitos de titulares de dados; e te ensinar, passo a passo, como entrar em conformidade com o que ela estabelece. Ao final, você encontra um *checklist* para conferir se fez tudo direitinho, uma lista com indicações de sites para se atualizar sobre a nova legislação e pesquisar sobre a proteção de dados pessoais, e um glossário para consultar termos técnicos referentes à Lei.

Você vai ver que a adequação à LGPD é um movimento importante para preservar sua instituição e garantir os direitos dos/as titulares de dados que interagem com ela, além de ser uma oportunidade de rever e atualizar processos e fluxos institucionais.

Esperamos que este material te estimule e ajude a implementar a LGPD! Boa leitura!

1. PRIMEIRAS QUESTÕES

O QUE É MESMO A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)?

É como é chamada a Lei 13.709/2018, que foi elaborada para garantir um conjunto de direitos básicos relacionados aos dados pessoais, diante da crescente digitalização das mais diversas relações de consumo. Ela determina como, quando e por que empresas, organizações da sociedade civil e poder público podem tratar, armazenar e compartilhar dados das pessoas, desde informações pessoais até reações que podem ser monitoradas em ambiente digital. A LGPD entrou em vigor em 18 de setembro de 2020.

POR QUE ADEQUAR MINHA INSTITUIÇÃO?

Em primeiro lugar, é um compromisso com a privacidade das pessoas que fornecem algum tipo de informação para a sua organização. Além disso, você estará evitando incidentes de proteção de dados e, consequentemente, sanções judiciais ou regulatórias. Não menos importante é contribuir para a construção de uma cultura de proteção de dados e para o aperfeiçoamento contínuo das estruturas e processos criados para garantir o cumprimento da Lei.

QUAIS SÃO OS PRINCIPAIS PROCESSOS PARA IMPLEMENTAR A LGPD NA MINHA ORGANIZAÇÃO?

Governança de dados: inclui a revisão de políticas de privacidade e de termos de uso, além da garantia de condições de rastreabilidade dos processos de tratamento de dados pessoais, ou seja, a possibilidade de saber quando os dados foram coletados, para que e por quanto tempo ficarão armazenados.

Segurança da Informação: envolve a criação de mecanismos para assegurar a proteção dos bancos de dados mantidos pela organização, para evitar perda, alteração, comunicação ou difusão indevida e ilegítima das informações.

Atendimento aos/às titulares de dados: diz respeito à criação de mecanismos e fluxos para responder a possíveis requerimentos dos/as titulares de dados e da Autoridade Nacional de Proteção de Dados (ANPD), além

do destacamento de colaboradores/as para lidar com essas requisições e com os possíveis incidentes de proteção de dados, que podem ocorrer mesmo após um processo de conformidade com a Lei.

QUANTO TEMPO PODE LEVAR UM PROJETO DE ADEQUAÇÃO À LGPD?

É preciso ter cuidado ao generalizar, pois cada projeto de adequação é único. Mas, com base na nossa experiência, é possível pressupor que em micro e pequenas organizações - ou seja, em instituições com poucos/as colaboradores/as, com um volume relativamente pequeno de dados ou fluxos pouco intensos de tratamento - o processo de adequação pode durar aproximadamente 3 meses, dependendo do risco envolvido nas suas atividades de tratamento. Em instituições maiores, esse tempo pode chegar a 1 ano.

2.

VERDADES SEJAM DITAS

Uma nova legislação sempre gera dúvidas, às vezes até insegurança, e, nesse contexto, é comum circularem ideias e informações falsas. A seguir, comentamos alguns dos principais pontos que geram dúvidas, para você não espalhar nem cair em *fake news*.

SUA ORGANIZAÇÃO DEVE, SIM, SE ADEQUAR À LGPD, MESMO QUE NÃO ATUE COM DADOS SENSÍVEIS, NÃO ATENDA DIRETAMENTE PESSOAS FÍSICAS, NEM SEJA DO RAMO DA TECNOLOGIA

A Lei se aplica ao tratamento de qualquer dado pessoal, mesmo que seja apenas o e-mail ou o CPF, de qualquer pessoa física, mesmo que ela represente uma empresa. Então, se uma instituição capta e armazena dados pessoais, ela deve se adequar à LGPD, independente do seu ramo de atuação.

Por exemplo, se sua organização tem colaboradores/as ou associados/as, todos os dados coletados com a finalidade de possibilitar o desenvolvimento da relação de trabalho são dados pessoais e, por isso, precisam estar protegidos pelos mecanismos previstos na Lei.

O PROCESSO DE ADEQUAÇÃO À LEI NÃO PRECISA SER CARO E DEVE SE ADAPTAR À SUA REALIDADE

Não pense que, porque sua organização é pequena, ela não terá condições de cumprir o que a LGPD exige. Na verdade, o processo de adequação à Lei é bastante específico para cada instituição e deve ser feito sob medida para sua realidade.

Para baratear a adequação, os procedimentos podem ser conduzidos por advogados/as autônomos/as que já possuem alguma experiência com proteção de dados. Além disso, existem escritórios e profissionais que vendem serviços de adequação por etapas ou dão consultoria para que a própria equipe da instituição possa mapear os fluxos e organizar estruturas de proteção de dados, realizando apenas um monitoramento desse processo. Também já existem diversos cursos e treinamentos, gratuitos e pagos, realizados online ou de forma presencial para quem quer se capacitar.

Ainda pensando em economia, vale lembrar que a implementação da LGPD é um investimento nos processos e estruturas de dados da organização,

que, além de garantir a adequação às exigências legais, poderá aumentar a eficiência da sua instituição.

De quebra, você aumenta suas possibilidades de investimento e parcerias com empresas e instituições filantrópicas estrangeiras que já tenham se adequado à legislação de proteção de dados europeia, por exemplo, e que exigem que parceiros implementem programas de governança de dados e segurança da informação.

Além de tudo isso, entendemos que a proatividade no processo de adequação à Lei, sem esperar que aconteçam incidentes e violações, é um ato de comprometimento, por parte de organizações, com os princípios gerais de privacidade e proteção de dados pessoais e que será valorizado por consumidores/as e parceiros/as igualmente comprometidos com esse tema.

VOCÊ PODE IMPLEMENTAR A LEI COM A ESTRUTURA JÁ EXISTENTE NA SUA ORGANIZAÇÃO, NÃO É NECESSÁRIO UM SETOR DE TECNOLOGIA DA INFORMAÇÃO

A maioria das diretrizes previstas na LGPD tem a ver com efetivar o direito à informação de titulares de dados pessoais e com garantir que existam medidas de proteção dos dados fornecidos quando acessam seu serviço ou produto.

Muitas dessas diretrizes podem ser efetivadas demonstrando o caminho que os dados de usuários/as percorrem dentro da sua instituição e a maneira como eles são utilizados, armazenados e com quem são compartilhados. Sempre garantindo e deixando clara a relação entre a finalidade declarada na hora da coleta das informações e a finalidade concreta do uso. E você pode fazer isso com ajuda de advogados/as ou escritório terceirizado que oriente sua equipe.

É verdade que, para formular algumas das medidas de Segurança da Informação, você precisará de auxílio profissional, pois, muitas vezes, é necessário implementar *softwares* ou rotinas de proteção mais eficientes e robustos. Porém, é possível começar o processo sem ter um setor de Tecnologia da Informação (TI) e se - e quando - for necessário, contar com serviços terceirizados, adequados ao tamanho da sua organização e à quantidade de

dados processados por ela. Também há profissionais de TI autônomos/as que fazem preços amigáveis ou atuam de forma gratuita em coletivos de profissionais dessa área.

No Idec, temos uma equipe dedicada a monitorar a segurança e cuidar do armazenamento dos nossos bancos de dados.

O OBJETIVO DA LEI DE PROTEÇÃO DE DADOS É PREVENIR VAZAMENTOS E PROMOVER A RESPONSABILIZAÇÃO QUANDO ISSO OCORRER, E NÃO QUEBRAR ORGANIZAÇÕES COM SUAS MULTAS

Muitas instituições andam assombradas com a multa de até 2% sobre o faturamento, prevista na LGPD. Porém, é importante saber que a legislação tem sanções gradativas e limitadas ao porte da organização. Esse limite é fixado em relação ao faturamento da Pessoa Jurídica em questão - e, para se ter uma ideia, é de R$2.000,00 no caso de microempresas com faturamento de até R$100.000,00 por ano. O caso das organizações sem fins lucrativos não está especificado na Lei e deve ser regulamentado posteriormente.

Além disso, a quebra das regras da LGPD não implica uma multa imediata; antes, são aplicadas penalidades mais leves, como: advertência com indicação de prazo para adoção de medidas corretivas, publicização da infração após apuração do que ocorreu, bloqueio temporário dos dados pessoais envolvidos na infração ou determinação de sua eliminação. O início da aplicação das sanções previstas na Lei para as empresas que desrespeitarem suas regras é 1º de agosto de 2021.

Viu como não precisa ter medo? O importante é se preparar e se precaver, já que as sanções dependem dos efeitos do incidente de proteção de dados ou da falta de medidas para evitá-lo.

VOCÊ NÃO PRECISA COLETAR O CONSENTIMENTO DE TITULARES DE DADOS PARA TODA AÇÃO ENVOLVENDO SEUS DADOS

É verdade que a LGPD estabelece que é preciso ter justificativas legais para coletar e tratar dados pessoais, mas ter o consentimento de titulares é apenas uma das 10 justificativas previstas na Lei - você vai conferir

todas elas na parte 3 deste Manual. Ou seja, há casos - como quando o tratamento dos dados for uma condição para cumprimento de obrigações legais ou para execução de políticas públicas - em que o consentimento do/a titular não é necessário.

Vale registrar que, no caso das relações de trabalho, o consentimento não é necessário pois não é sequer considerado uma justificativa válida, já que se considera que a grande assimetria das relações entre empregadores/as e colaboradores/as ou candidatos/as a vagas de trabalho tende a interferir na obtenção do consentimento.

A LGPD NÃO IMPEDE QUE VOCÊ MONITORE AS PESSOAS QUE TRABALHAM NA SUA INSTITUIÇÃO OU REQUISITE OS SEUS ANTECEDENTES CRIMINAIS QUANDO ISSO FOR JUSTIFICÁVEL

O monitoramento de colaboradores/as não é proibido, mas, com a aplicação da Lei, as pessoas devem conhecer o funcionamento e a finalidade desse monitoramento. Antecedentes criminais podem ser solicitados em casos específicos já identificados pela Justiça do Trabalho, como para as posições de motorista, trabalhadores/as que atuam com substâncias tóxicas ou com informações sigilosas, entre outras.

3.

CONHECENDO MELHOR A LGPD

Como vimos até aqui, a Lei Geral de Proteção de Dados não é um monstro que ameaça seu modelo de atuação, e a adequação das organizações da sociedade civil ao que ela estabelece é perfeitamente possível e irá beneficiar o conjunto da sociedade. Agora é hora de se familiarizar com os principais conceitos dessa legislação, para aplicá-la com segurança.

Para começar, vamos responder algumas questões sobre termos importantes que você vai encontrar. Talvez você esteja se fazendo essas perguntas!

O QUE SÃO DADOS PESSOAIS E QUAL A DIFERENÇA EM RELAÇÃO AOS DADOS SENSÍVEIS? O QUE SIGNIFICA ANONIMIZAÇÃO?

Dados pessoais são quaisquer informações que possibilitem a identificação de alguém, por exemplo: telefone, endereço, CPF, link de perfil em redes sociais, entre outros.

Já os **dados sensíveis** são informações sobre aspectos da vida de alguém que podem gerar situações delicadas, como algum tipo de discriminação ou exposição. A partir da Lei, consideram-se sensíveis os seguintes dados: orientação sexual; orientação religiosa; filiação política ou partidária; raça; dados de saúde, genéticos e biométricos. Destacamos que a Lei não menciona explicitamente orientação sexual ou identidade de gênero como dado sensível, mas, devido ao potencial discriminatório dessas informações, recomendamos tratá-las como dados sensíveis, conferindo maior nível de proteção.

É aí que entra a tão falada **anonimização**, um procedimento por meio do qual a ligação entre o/a titular de dados e as informações sobre ele/a é quebrada, impedindo sua identificação a partir dos dados retidos por uma instituição.

Por exemplo, se sua organização solicita o dado racial de candidatos/as a vagas de trabalho, com a justificativa legal de criar uma estatística sobre a efetividade da contratação de pessoas não brancas, você precisa garantir a anonimização desse dado na publicação da estatística, não mencionando as pessoas e suas raças autodeclaradas, mas apenas os valores agregados.

Ou, ainda, se sua organização pretende fazer um balanço sobre a diversidade de perfis de funcionários/as, é preciso prestar atenção à anonimiza-

ção de dados ao cruzá-los com outras informações. Por exemplo, se for comunicar informações salariais com recorte de raça e de gênero e houver apenas uma mulher negra na sua equipe, fica fácil identificar a pessoa e, com isso, vazar uma informação sigilosa.

O QUE SIGNIFICA TRATAMENTO DE DADOS?

Tratamento de dados é tudo aquilo que pode ser feito com uma informação, desde o momento em que ela entra no seu banco de dados até ser excluída dele. Por exemplo: coletar, armazenar, transferir, formular, analisar, inserir em planilhas, realizar monitoramento ou publicidade a partir das informações, etc. Tudo isso é tratamento de dados. Ou seja, é praticamente impossível que uma instituição, seja qual for seu tamanho ou área de atuação, não faça tratamento de dados!

Outra possibilidade de tratamento é o uso compartilhado de dados, que se refere à comunicação, difusão, transferência internacional ou tratamento compartilhado de bancos de dados pessoais, com autorização específica, entre entes públicos ou privados. Nesse caso, ambas as instituições devem se responsabilizar pelos direitos de titulares.

QUAL A DIFERENÇA ENTRE CONTROLADOR/A, ENCARREGADO/A E OPERADOR/A?

Controlador/a é a pessoa física ou jurídica que pode ser identificada como responsável pelas decisões sobre a finalidade do tratamento de dados, o meio de captação e os fluxos envolvendo tais informações.

A LGPD exige que o/a controlador/a nomeie um/a **Encarregado/a** pelas atividades de tratamento de dados pessoais da instituição. Também conhecido/a como encarregado/a de proteção de dados ou DPO (Data Protection Officer), é a pessoa responsável pelo contato com a Autoridade Nacional de Proteção de Dados (ANPD) e com os/as titulares de dados, atendendo suas demandas.

Operador/a é a pessoa física ou jurídica que realiza o tratamento de dados a mando do/a controlador/a, segundo suas diretrizes.

No caso do Idec, temos parceria com uma empresa de Tecnologia da Informação, que cuida dos processos de armazenamento e segurança dos nossos bancos de dados. Nesse caso, essa empresa é a operadora, o Idec é o controlador desses dados e temos uma pessoa da equipe que é a encarregada.

COMO OCORRE A RESPONSABILIZAÇÃO DOS/DAS CONTROLADORES/AS POR INCIDENTES DE PROTEÇÃO DE DADOS?

Segundo a LGPD, um tratamento de dados é considerado irregular ou ilícito quando o/a controlador/a deixa de observar os parâmetros legais sobre: a finalidade do tratamento; ou o resultado e os riscos envolvidos; ou as técnicas utilizadas.

Para que se caracterize um incidente de proteção de dados, é preciso que se evidencie:

- quem são as pessoas prejudicadas ou vítimas;
- qual dano elas sofreram; e
- a ligação entre o dano e as condutas do/a agente de tratamento de dados (controlador/a e/ou operador/a).

Quando há mais de uma instituição envolvida no tratamento de dados em questão, todas elas podem ser chamadas a responder pelo incidente, uma vez que a responsabilidade pelo dano é compartilhada.

Para se defender da responsabilidade pelo ocorrido, o/a controlador/a das informações deve provar:

- que não realizou o tratamento de dados irregular que lhe está sendo atribuído; ou
- que realizou o tratamento, mas que ele não viola a legislação de proteção de dados; ou
- que a responsabilidade é exclusiva de terceiros/as ou dos/as próprios/as titulares de dados.

Caso nenhuma dessas situações seja provada, o/a controlador/a terá a obrigação de reparar os possíveis danos gerados por sua conduta.

Mas é importante lembrar que o/a operador/a também poderá ser responsabilizado/a, caso não tenha seguido instruções lícitas do/a controlador/a ou se tiver desrespeitado a legislação de proteção de dados. Ou seja, será preciso verificar se as instruções presentes nos documentos que orientam a proteção dos dados da instituição, ou das instituições envolvidas, foram seguidas por todas as partes no tratamento de dados que está sendo questionado.

É importante dizer, também, que a Autoridade Nacional de Proteção de Dados (ANPD), para aplicar as sanções previstas na LGPD, levará em consideração se a organização criou mecanismos para evitar e para responder com agilidade a possíveis incidentes de dados. Caso a instituição não tenha se adequado à Lei, a sanção ou multa aplicada ao/à controlador/a pode ser mais grave.

Percorrendo a Lei

Agora vamos percorrer as partes da Lei, usando como metáfora a construção de uma casa!* A casa pronta é uma instituição já adequada à LGPD, então, antes da adequação, sua organização tem apenas o terreno, que são os dados pessoais recolhidos e armazenados por ela.

A estrutura dessa construção são os princípios que guiam a aplicação da Lei, desde sua implementação até eventuais sanções por falhas na proteção de dados. Assim como é importante uma casa ter estruturas sólidas, conhecer os princípios da Lei te dará segurança para aplicá-la.

As paredes são as bases legais que permitem que você utilize os dados pessoais que captou para a finalidade que precisa no seu trabalho. Na casa, as paredes sustentam o teto; no processo de adequação, a conformidade com as bases legais garante os direitos de titulares. Portanto, a cobertura dessa casa são os direitos exercidos por titulares de dados.

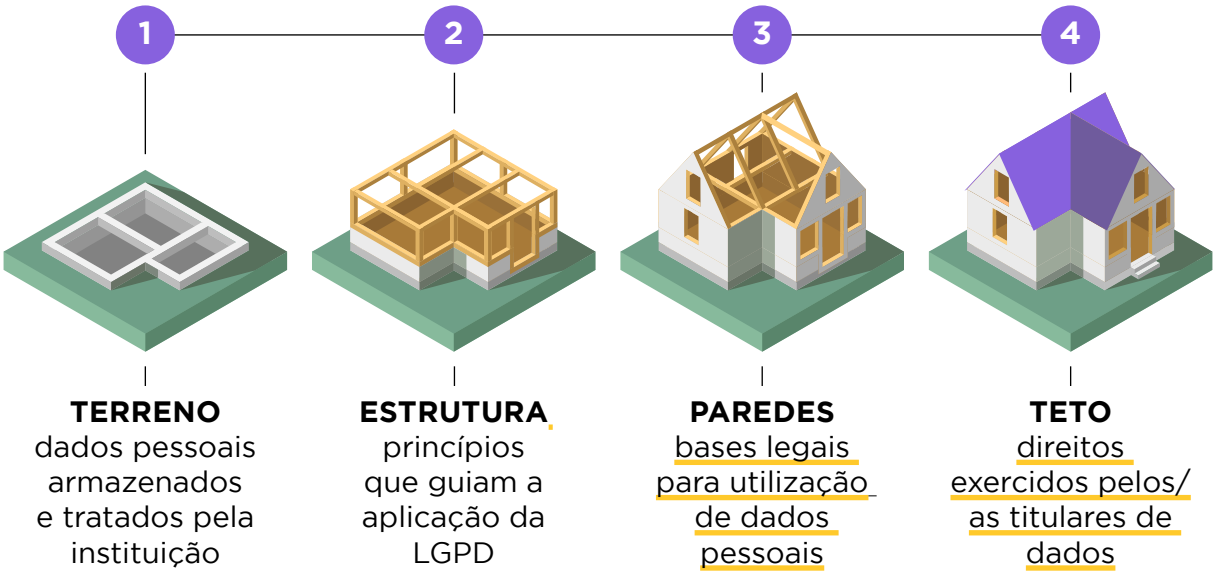
* Metáfora utilizada pela advogada Mariana de Toledo durante o curso “LGPD 4.0.”.

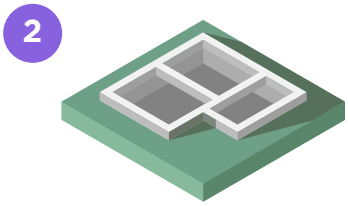
Um teto protege de sol, chuva e sereno; já os direitos estabelecidos pela LGPD protegem contra vazamentos e usos ilegítimos ou injustificados de dados pessoais, além de garantirem atendimento aos/às titulares de dados.

Ilustrando nossa metáfora:

Construção da casa // Adequação à LGPD

Este é o percurso para "construir"
uma organização adequada à LGPD





Fincando as estruturas: Princípios que guiam a aplicação da LGPD

Logo no primeiro capítulo da Lei temos os princípios que orientam sua correta aplicação. Isso quer dizer que, para se adequar à LGPD, é preciso respeitar essas diretrizes, que veremos a seguir.

FINALIDADE

Propósito legítimo, baseado na lei e informado ao/à titular, que assegura a legalidade do tratamento de seus dados. É o PARA QUE do tratamento de dados que sua organização realiza. Isso quer dizer que é preciso ter uma justificativa razoável para captar e utilizar dados pessoais. Essa finalidade da coleta e do uso dos dados deve ser informada ao/à titular no momento da captação de suas informações e, se for alterada, deve ser comunicada novamente. Cada tipo de dado deve ter uma finalidade

específica que justifique seu tratamento, senão será considerado um tratamento inadequado.

Por exemplo, se você coleta nome e endereço eletrônico de visitantes do seu site para continuar a comunicação por e-mail, sua finalidade é o envio de conteúdo, mas lembre-se de pedir o consentimento para isso.

NECESSIDADE

O princípio da necessidade está ligado ao da finalidade no sentido de que você só pode coletar os dados que forem indispensáveis para realizar a finalidade informada. Ou seja, não vale mais a lógica que diz "quanto mais dados, melhor".

Por exemplo, para coletar inscrições em eventos, é razoável solicitar nome, e-mail e número de celular, pois essas informações são necessárias para confirmar participações, informar, identificar e até certificar participantes. Então, caso não haja justificativa, você não poderá solicitar dados sobre a orientação sexual, raça, geolocalização, entre outros, que são desnecessários para viabilizar a participação no evento.

ADEQUAÇÃO

Diz respeito à necessidade de buscar os meios mais adequados para realizar a coleta e o tratamento de informações pessoais. Por exemplo, pode não ser adequado exigir que o/a titular forneça dados pessoais para acessar - digital ou presencialmente - conteúdos básicos como os serviços oferecidos pela sua organização e o seu modo de atuação. O ideal é que o acesso a esse tipo de informação seja livre.

LIVRE ACESSO

Segundo esse princípio, sua instituição deve garantir o acesso de titulares de dados às informações fornecidas a ela. Será preciso criar um fluxo e disponibilizar pessoas para lidar com essa demanda, considerando que a consulta nunca poderá ser cobrada e o modo de acesso aos dados deve estar exposto de forma clara no seu site ou nas paredes da sede, por exemplo, de forma que a pessoa não tenha dificuldade para fazer isso, caso deseje.

QUALIDADE DE DADOS

Toda instituição que capta dados pessoais deve garantir que as informações mantidas em sua base de dados sejam o mais fidedignas possível. Isso

quer dizer que elas devem estar sempre atualizadas, corretas e coerentes com a realidade.

Nesse sentido, é importante pensar em mecanismos ativos e passivos de atualização. Ou seja, sua organização deve atualizar os dados regularmente e, também, disponibilizar canais para que o/a titular possa fazer atualizações de maneira descomplicada. Dificultar ou burocratizar o acesso aos dados é sinal de má fé.

TRANSPARÊNCIA

É uma condição para que titulares de dados exerçam seus direitos e, portanto, uma obrigação das instituições que recolhem dados pessoais. Ser transparente significa prestar contas sobre como sua instituição trata os dados que ela recolhe e mantém, tanto para os/as titulares quanto para seus parceiros e para a Autoridade Nacional de Proteção de Dados (ANPD), que representa o interesse público.

SEGURANÇA

Os dados coletados por sua instituição devem estar protegidos e só podem ser acessados pelas pessoas e para as finalidades informadas aos/às titulares no momento da coleta. Ou seja, não podem vazar.

Em muitos casos, como quando a organização trabalha com grupos socialmente vulnerabilizados, vazamentos de dados podem implicar em discriminação e perseguição, tanto *online* quanto *offline*. É importante criar níveis diferenciados de proteção para esses casos específicos, limitando as pessoas que têm acesso a essas informações. Lembre-se que muitos incidentes de vazamento de dados têm causas internas, então é fundamental que sua equipe tenha um treinamento adequado sobre Segurança da Informação.

PREVENÇÃO

Esse princípio está ligado ao anterior, pois é responsabilidade das instituições adotarem, de forma preventiva, medidas de segurança dos dados para evitar que aconteça qualquer incidente.

NÃO DISCRIMINAÇÃO

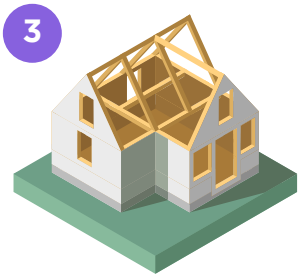
As informações pessoais que sua instituição possui, especialmente os dados sensíveis, não podem ser utilizados para promover qualquer tipo de discriminação. Ou seja, os dados das pessoas não podem ser usados

para tratá-las de forma desigual, por exemplo, em função de características como idade, gênero, raça ou orientação sexual.

PRESTAÇÃO DE CONTAS

Esse princípio está ligado ao da Transparência. Sua organização precisa documentar os fluxos de informações, demonstrando, basicamente: como os dados entram na instituição, qual finalidade justifica essa entrada, com quem os dados são compartilhados, a finalidade do compartilhamento, o modo de armazenamento e a forma de exclusão das bases de dados. É isso que os/as titulares de dados pessoais, seus parceiros e a ANPD têm direito de saber.

3



Erguendo as paredes: Bases legais para o tratamento de dados

O que chamamos de "bases legais de tratamento de dados pessoais" são as justificativas previstas na Lei que permitem que você faça a captação e o tratamento de informações pessoais de quem interage com a sua instituição. Você deve informar essas razões ao/à titular no momento da coleta de seus dados.

A LGPD traz 10 possibilidades legítimas de tratamento de dados pessoais. A seguir, vamos entender um pouco melhor o que é consentimento e quais são as finalidades que podem legitimar o tratamento de dados, de acordo com a Lei.

CONSENTIMENTO

Essa é a mais conhecida base legal de tratamento de dados que a Lei traz. O consentimento é quando o/a titular de dados autoriza o uso de seus dados.

A solicitação de consentimento não é só um pedido de "tique" em uma caixinha que diz "Li e aceito". É preciso usar a criatividade e as tecnologias para garantir e documentar que a pessoa entendeu perfeitamente a finalidade do uso dos seus dados e o autorizou livremente.

A LGPD diz que o consentimento deve ser exposto em CLÁUSULA DESTACADA, ou seja, em uma parte separada e impossível de não ser vista

no aviso sobre a finalidade do uso dos dados. De modo geral, a opção pelo consentimento como base legal deve ser priorizada em relação às outras justificativas de tratamento que a Lei traz.

Para dados manifestamente públicos, ou seja, que estão disponíveis em bases do governo, como salários de funcionários/as do setor público, o consentimento é dispensado, porém continua sendo necessário justificar o tratamento com uma das outras bases legais. Ainda há discussão sobre se perfis e *posts* de redes sociais são considerados dados públicos. O tratamento desses dados deve ser feito, então, mediante a informação quanto à finalidade do uso e o consentimento do/a titular.

No caso de dados sensíveis, o consentimento só será dispensado se houver outra base legal imprescindível, como a proteção da vida do/a titular. Por exemplo: apesar de informações de saúde serem consideradas dados sensíveis, se a organização precisar coletá-las para evitar que uma pessoa assuma funções que possam agravar doenças preexistentes, o consentimento poderá ser dispensado.

OBRIGAÇÃO LEGAL

A justificativa de obrigação legal pode ser utilizada quando você está tratando dados com a permissão ou por imposição de outra lei ou norma, como um regulamento ou portaria administrativa.

É, normalmente, o caso dos dados utilizados para a contratação e manutenção de uma relação de trabalho, que, quase em sua totalidade, são coletados por conta de obrigações da legislação trabalhista ou previdenciária.

Porém, o uso da obrigação legal como justificativa para o tratamento de dados só pode acontecer dentro do prazo que o/a titular de dados tem para entrar com uma eventual ação contra sua instituição, por conta da relação estabelecida no momento da coleta de dados, por exemplo, a prestação de um serviço. Esse período pode variar, dependendo se é uma ação civil, penal ou administrativa. Para saber qual é o seu caso, é importante consultar um/a advogado/a.

EXECUÇÃO DE POLÍTICAS PÚBLICAS

Essa base legal só é utilizada, praticamente, por órgãos e instituições públicas. Para justificar o tratamento de dados, as políticas públicas devem

estar previstas em leis ou regulamentos ou respaldadas por contratos, convênios ou outros instrumentos normativos do gênero.

Sua organização, por exemplo, poderia utilizar essa justificativa no âmbito de uma parceria público-privada, para captar os dados necessários à elaboração e implementação da política pública a ser desenvolvida a partir dessa parceria.

REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA

A justificativa de utilização dos dados captados para fins de pesquisa só pode ser utilizada por órgãos e instituições que tenham como objeto social, no CNPJ, a realização de pesquisas, seja em conjunto ou não com outras finalidades da instituição. Alguns exemplos de instituições conhecidas pelas pesquisas que produzem são a Fundação Getúlio Vargas ou o Instituto de Pesquisa Econômica Aplicada (IPEA).

EXECUÇÃO DE UM CONTRATO ASSINADO PELO/A TITULAR DE DADOS

Essa base legal pode ser utilizada para justificar a captação de dados que são necessários para cumprir uma obrigação assumida contratualmente pelo/a controlador/a com o/a titular de dados.

Por exemplo, para viabilizar a utilização de determinados serviços previstos em um contrato de plano de saúde, pode ser que o controlador - no caso, o plano de saúde - precise coletar dados sobre doenças preexistentes da pessoa que contratou o serviço. Aqui, o tratamento de dados é legítimo pois sem ele o serviço não poderia ser oferecido ao/à consumidor/a.

EXERCÍCIO REGULAR DO DIREITO EM PROCESSOS

Essa justificativa permite que um/a titular de dados ou uma pessoa jurídica acesse informações armazenadas por instituições para compor um processo judicial ou administrativo que pretenda mover contra terceiros/as. Ela é importante porque dispensa o consentimento da parte contrária, desde que as informações sejam fundamentais para o desenvolvimento do processo.

Por exemplo, para defender os interesses de consumidores/as associados/as, o departamento jurídico do Idec capta dados necessários para mover Ações Civis Públicas ou privadas.

PARA A PROTEÇÃO DA VIDA OU INCOLUMIDADE DO/A TITULAR OU DE TERCEIRO/A

Essa base legal permite a utilização de dados pessoais para a proteção de pessoas que estejam em risco de vida ou de violência física. Nessas situações, é possível utilizar até dados sensíveis, como gênero e raça, para preservar a segurança física do/a titular.

Por exemplo, é legítimo que uma casa de acolhimento à população LGBTQI+ utilize dados de pessoas que sofrem violência ou perseguição por serem transsexuais/transgêneras, para oferecer a elas um abrigo seguro.

PARA A TUTELA DE SAÚDE

Essa justificativa só pode ser usada por profissionais, serviços ou autoridades da área da saúde, para viabilizar tratamentos e serviços que visam a saúde do/a titular de dados.

Por exemplo, quando uma pessoa precisa de uma cirurgia de urgência, é legítimo que órgãos de saúde forneçam seu histórico médico para possibilitar tal atendimento.

PARA A PROTEÇÃO DO CRÉDITO

Essa é a justificativa legal que permite que instituições financeiras tratem os dados dos/as titulares para protegerem o crédito que vão fornecer, ou seja, para evitarem "calote".

EM RAZÃO DO LEGÍTIMO INTERESSE DO/A CONTROLADOR/A

Muitas vezes essa justificativa é vista como um coringa e tem sido usada quando o interesse por trás do tratamento de dados não pode ser defendido por nenhuma das outras justificativas previstas na Lei. Mas, alertamos que essa utilização NÃO É RECOMENDADA.

Se não é possível justificar algum procedimento que sua organização realiza utilizando nenhuma das outras 9 bases legais previstas, talvez seja o caso de repensar a real necessidade desses dados para o desenvolvimento de suas atividades.

Para te ajudar a saber se seu caso é um caso de legítimo interesse do/a controlador/a, sugerimos que siga os passos abaixo. Para usar essa justificativa, sua instituição deve conseguir cumprir todos esses requisitos:

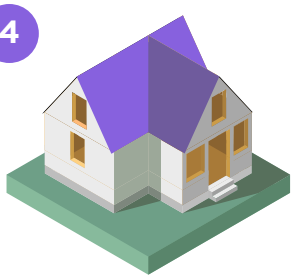
- Identificar se o que sua instituição deseja fazer com os dados é legal, ou seja, se não existe alguma proibição dessa finalidade na legislação brasileira;

- Indicar, com clareza, a real necessidade do tratamento das informações, considerando a finalidade que você tem;

- Entender se as expectativas da instituição e as dos/as titulares, em relação à finalidade do uso dos dados, estão alinhadas, ou seja, se ambas as partes entendem que o tratamento é importante para alcançar interesses comuns;

- Fornecer, aos/às titulares, mecanismos de proteção dos dados captados, garantindo que possam se opor de forma justificada a tratamentos que considerem indevidos, exercendo assim seus direitos.

4



Cobrindo sua casa: Direitos dos/as titulares de dados

É chegada a hora de cobrir "nossa casa". É importante que a estrutura e as paredes estejam sólidas, pois o teto dessa construção são os direitos de titulares de dados, que, para serem garantidos, dependem da compreensão dos princípios da Lei e da aplicação de suas bases legais.

A efetivação desses direitos depende, ainda, da criação de um canal direto de contato entre titulares e encarregado/a de proteção de dados da sua organização, que é quem atenderá as solicitações que aparecerem.

A seguir, você vai ver os direitos que precisam ser garantidos a todas as pessoas que se relacionam de alguma forma com sua instituição, sejam beneficiários/as, colaboradores/as, doadores/as, parceiros/as, voluntários/as, fornecedores/as, etc.

DIREITO À CONFIRMAÇÃO de que a sua organização realiza tratamento de dados. Essa confirmação, solicitada pelo/a titular, pode ser dada, de imediato, pela instituição, em formato simplificado - por exemplo, com um aviso informando a finalidade e duração do armazenamento e tratamen-

to dos dados - ou em até 15 dias, por meio de declaração completa que indique origem dos dados, existência de registro, critérios utilizados para captação e finalidade do tratamento.

DIREITO DE ACESSO AOS DADOS que sua instituição armazena. Ou seja, titulares de dados podem solicitar uma lista com os dados que você retém sobre eles/as. Por isso, é importante mapear o fluxo das informações dentro da sua organização, assim você não terá dificuldade para encontrá-las.

DIREITO DE CORRIGIR DADOS incompletos, inexatos ou desatualizados.

DIREITO DE EXERCER A PORTABILIDADE DOS DADOS PESSOAIS que sua instituição armazena, podendo levá-los para outra instituição, após realizar uma requisição ao/à encarregado/a de proteção de dados da sua organização.

DIREITO DE REQUISITAR A ELIMINAÇÃO DE DADOS PESSOAIS tratados com base no consentimento, o que deverá ser feito a não ser que a instituição justifique a manutenção do tratamento por conta de cumprimento de uma obrigação legal, estudo por órgão de pesquisa, transferência para terceiros/as ou uso exclusivo do/a controlador/a. Lembramos que, neste último caso, os dados devem ser anonimizados e ter seu acesso vedado a terceiros/as.

DIREITO DE SER INFORMADO/A QUANTO AO COMPARTILHAMENTO de seus dados com entidades públicas ou privadas, independente de solicitar ou não essa informação. Lembrando que o compartilhamento com terceiros/as é vedado no caso de tratamento de dados para uso exclusivo do/a controlador/a.

DIREITO DE SER INFORMADO/A SOBRE A POSSIBILIDADE E AS CONSEQUÊNCIAS DE NÃO FORNECER O CONSENTIMENTO, no momento de sua solicitação, quando essa for a base legal que justifica a coleta dos dados.

DIREITO DE REVOGAR O CONSENTIMENTO a qualquer momento.

4.

ADEQUAÇÃO NA PRÁTICA – PASSO A PASSO

Agora você já sabe o que é a Lei Geral de Proteção de Dados e por que deve implementá-la na sua organização. Então vamos ver como a adequação à Lei acontece na prática!

Existem diversas metodologias, mas, se você trabalha em uma Organização da Sociedade Civil, pode ser que elas não sejam adequadas para o seu caso, por não fazerem sentido para sua realidade. No caso de instituições pequenas, por exemplo, algumas etapas do processo de adequação podem ocorrer simultaneamente, em momentos ou em ordem diferentes do que normalmente é sugerido.

A seguir, sugerimos 7 passos básicos, que você pode adaptar ao contexto da sua organização.

1º PASSO: DEFINIR O PRINCIPAL OBJETIVO DA ADEQUAÇÃO

2° PASSO: CONSCIENTIZAR E CAPACITAR A EQUIPE SOBRE A LGPD

3º PASSO: CONTRATAR SERVIÇO DE CONSULTORIA OU IMPLEMENTAÇÃO

4° PASSO: MAPEAR FLUXOS DOS DADOS

5° PASSO: MELHORAR DOCUMENTOS E FLUXOS

6° PASSO: REDIGIR OS DOCUMENTOS DE PROTEÇÃO DE DADOS

7º PASSO: DEFINIR O/A ENCARREGADO/A DE DADOS

Vamos entender melhor cada um deles?

1º PASSO: DEFINIR O PRINCIPAL OBJETIVO DA ADEQUAÇÃO

A primeira coisa que você precisa fazer é responder à questão: qual objetivo vai guiar seu processo de adequação à LGPD, além de cumprir obrigações legais e evitar multas e sanções?

Cada organização terá um foco específico, ou seja, um propósito ligado às suas atividades, à sua estrutura ou ao momento institucional, além da imposição de se adequar à Lei, como todas as outras instituições, independente de natureza, área ou porte.

Por se tratar de uma definição institucional estratégica, este é um momento privilegiado para engajar a gestão da organização no processo de adequação, caso isso ainda não tenha acontecido. O comprometimento das lideranças é fundamental para garantir os recursos humanos e financeiros necessários, além de ser um exemplo para o restante da equipe.

No caso de OSCs, um dos pontos que pode ser levado em consideração na definição desse objetivo é o fato de que se adequar à LGPD contribui para a transparência da instituição, o que pode ter impactos positivos na imagem e no potencial de captação de recursos, além de favorecer o estabelecimento de parcerias com o poder público ou com fundações e empresas, inclusive estrangeiras, que exigem boas práticas de governança.

Outro tema muito relevante para organizações sociais é a sensibilidade dos dados manejados. Ao definir seus objetivos, considere se a atuação da instituição pode vir a ser objeto de perseguição político-ideológica ou se o público com o qual ela interage é formado por pessoas que podem vir a sofrer discriminações ou violências em função de características ou posicionamentos expressos em seus dados pessoais.

Já vimos que informações sobre o posicionamento político, a orientação sexual e a raça do/a titular, entre outros, são considerados dados sensíveis e, por isso, evitar seu vazamento deve ser uma prioridade. Abaixo relacionamos alguns objetivos associados a isso, como referência:

- Proteger dados sensíveis com mecanismos administrativos e técnicos de Segurança da Informação, criando fluxos especiais de compartilhamento;

- Estabelecer métodos seguros de armazenamento e descarte das informações dos/as titulares de dados de grupos socialmente vulneráveis;

- Restringir e definir finalidades claras para captação e compartilhamento de dados, atrelando o tratamento às atividades realizadas pela instituição, com base nas justificativas que a Lei traz.

Por fim, mas não menos importante, sobretudo para organizações que atuam com a defesa de direitos, é preciso considerar que a implementação da LGPD também está ligada à proteção de interesses e liberdades das pessoas que interagem com a sua instituição.

2° PASSO: CONSCIENTIZAR E CAPACITAR A EQUIPE SOBRE A LGPD

Mesmo que sua organização defina pessoas específicas para tratar dados pessoais, é importante que todas as pessoas da sua equipe sejam apresentadas aos principais conceitos da Lei, seus princípios, justificativas para tratamento de dados, direitos dos/as titulares e possíveis sanções.

Dessa forma, você estará criando uma cultura de proteção de dados, que tornará processos e rotinas institucionais sólidas, além de conscientizar seus/suas colaboradores/as sobre privacidade para que também possam exercer seus direitos, já que todos/as somos titulares de dados.

É importante ter em mente que esse passo não se encerra quando começar o próximo! A capacitação da equipe é um processo constante, que deve continuar durante toda a adequação e depois dela. Estabeleça os melhores momentos para isso, de acordo com a sua estrutura, e torne a proteção de dados um tema de formação permanente.

3º PASSO: CONTRATAR SERVIÇO DE CONSULTORIA OU IMPLEMENTAÇÃO

Como explicamos na parte 2 deste manual, existem escritórios ou advogados/as autônomos/as especializados/as na implementação da LGPD.

Vale a pena pesquisar seus pacotes de serviços, lembrando que, para baratear o processo, você também pode contratar serviços avulsos ou por etapas. Outra opção é contratar uma consultoria, para que sua própria equipe assuma as demandas de adequação à Lei, contando com formação e acompanhamento de especialistas.

Esse apoio será fundamental no próximo passo, para analisar as lacunas do seu atual fluxo de dados e propor ajustes, mas talvez seja interessante contar com esses/as profissionais já na definição dos seus objetivos e/ou para a capacitação inicial da equipe (passos 1 e 2). No Idec, por exemplo, o consultor contratado nos apoiou desde o começo, inclusive fazendo formações com a equipe para gerar uma mobilização interna em torno do tema.

Para te ajudar a escolher os serviços que irá contratar, listamos a seguir as tarefas que essa empresa ou profissional pode realizar no processo de adequação à LGPD da sua organização:

- Conscientização da equipe: mesmo que você decida contratar uma consultoria depois de já ter iniciado a formação interna sobre proteção de dados pessoais, aproveite os conhecimentos e experiências de especialistas para reforçar conceitos da Lei e esclarecer dúvidas da sua equipe. Lembre-se, a conscientização é um processo permanente!

- Capacitação do/a encarregado/a de dados: deve ser mais aprofundada, já que, quando o processo de adequação for concluído, é esse/a profissional que poderá tirar dúvidas e apoiar seus/suas colegas. Por isso, é importante que os/as especialistas o/a orientem mais de perto.

- Análise dos fluxos de dados da sua instituição e proposta de ajustes: depois de mapear os atuais instrumentos e processos ligados à captação e tratamento de dados na instituição, é interessante contar com o olhar de especialistas para identificar falhas e propor ajustes que deverão ser feitos durante a adequação à LGPD.

- Revisão de contratos e parcerias: a pessoa ou empresa contratada pode avaliar as situações em que sua instituição atua como

controlador/a ou operador/a e também os casos em que compartilha dados pessoais com terceiros/as. A partir daí, será possível entender as possibilidades de responsabilização da sua organização e projetar fluxos mais seguros com base na LGPD. Conte com os/as advogados/as especialistas que você contratar para formalizar esses acordos, revisando os contratos. Assim, sua instituição pode dar o exemplo e promover também a adequação de parceiros/as à legislação de proteção de dados.

- Criação de cláusulas e avisos sobre captação de dados: para estar em conformidade com a Lei, você precisará incluir cláusulas nos documentos ou outras plataformas utilizadas para captar dados pessoais, avisando os/as titulares sobre o uso que será feito dessas informações.

- Redação de documentos específicos da sua política de proteção de dados: além dos ajustes nos documentos que você já utiliza, será necessário elaborar novos documentos que consolidarão sua adequação à LGPD, como, por exemplo, Avisos de *Cookies* (rastreadores) e as Políticas de Privacidade e de Segurança da Informação. No 6º passo, detalhamos cada um desses instrumentos; aqui, o importante é saber que, para essa redação, você pode contar com os/as especialistas que contratar.

- Criação de listas de condutas (*checklists*): essas listas são um instrumento para que sua equipe avalie permanentemente se a estrutura de proteção de dados da sua organização está funcionando, e também para se orientarem em caso de dúvida sobre situações específicas.

- Monitoramento após a finalização do processo de adequação: sabemos que as maiores dúvidas só aparecem quando colocamos a mão na massa, ou seja, quando os/as colaboradores/as da sua organização começarem a aplicar a Lei no dia a dia de trabalho. Por isso, pode ser interessante combinar com os/as especialistas um período, após a adequação, em que eles/as poderão ser consultados/as para dúvidas e esclarecimentos e/ou para monitorar a aplicação dos mecanismos e práticas de proteção de dados pessoais.

4° PASSO: MAPEAR FLUXOS DOS DADOS

Chegou a hora de tirar uma espécie de fotografia de todos os processos que envolvem dados pessoais na sua instituição, desde a captação até o descarte. Ou seja, você deve colocá-los "no papel" de forma a identificar lacunas que podem ocasionar danos para os/as titulares e, consequentemente, penalidades para a organização. Por exemplo, o arquivamento de documentos sem data pode ser considerado uma lacuna, pois alguns tipos de dados possuem um prazo legal para serem descartados.

Para realizar o mapeamento de dados (*data mapping*), você deve se fazer as perguntas a seguir e registrar detalhadamente suas respostas:

- Como os dados pessoais entram na sua instituição?
- Por quais tratamentos cada tipo de dado passa em cada área ou projeto da instituição?
- Quais são as finalidades de cada informação coletada pela instituição? Todas são necessárias para o desenvolvimento das suas atividades?
- Há dados sensíveis? Quais?
- Há dados que são compartilhados? Quando e com quem?
- Como as informações são armazenadas e descartadas?

Uma sugestão é criar um formulário, físico ou digital, e pedir a todas as pessoas envolvidas no trajeto e tratamento dos dados pessoais, ou que são responsáveis por cada área ou projeto, que o respondam. A partir desse levantamento, conversas individuais ou em grupo podem ser marcadas para esclarecer dúvidas sobre os caminhos percorridos pelos dados dentro da organização. Quanto mais pessoas forem ouvidas, mais completo será o mapeamento.

Em instituições pequenas, a análise das lacunas pode acontecer junto com o mapeamento. Assim, você pode implementar medidas de segurança antes mesmo de terminar a redação da Política de Privacidade e o redesenho dos fluxos da instituição. Já no caso de instituições com um grande volume e/ou

complexidade de dados, a indicação é que o mapeamento seja finalizado antes de iniciar a análise das lacunas.

Uma boa opção para esse passo é utilizar ferramentas prontas para a criação de fluxos online, como o LucidChart e o Draw.io. A representação gráfica do seu mapa de dados pode ser usada nas conversas com a equipe, de forma que todos/as possam corrigi-lo ou melhorá-lo. Sugerimos que, ao final do processo de adequação, você atualize esses fluxos para ter um mapa do sistema de informações já adequado à LGPD.

5° PASSO: MELHORAR DOCUMENTOS E FLUXOS

Com o mapeamento do seu atual sistema de dados, o/a profissional que estiver realizando o processo de adequação à LGPD poderá identificar as vulnerabilidades quanto à proteção de dados e pensar em soluções adequadas para a sua realidade. Além disso, essa fotografia também permitirá que sejam identificadas as bases legais que podem justificar a captação e o tratamento de dados para as suas atividades.

Nesse momento você deve identificar e adequar os seguintes pontos:

Identificar	Adequar
Quais **documentos** são utilizados para captação de dados pessoais (fichas de cadastro, termos de voluntariado, etc.)	**Incluir cláusulas** sobre proteção de dados em todos.
Quais as **finalidades** dos tratamentos de dados pessoais feitos pela instituição (compartilhamento, análise, etc.)	**Eliminar a captação** de dados sem necessidade real para o desenvolvimento das suas atividades.
	Quando possível, **anonimizar** dados sensíveis ou que não precisam ter seus/suas titulares identificados/as.
	Elaborar justificativas para as coletas e tratamentos dos dados que serão mantidos, a partir das bases legais que a Lei traz.
	Definir o tempo de armazenamento dos dados e sua forma de exclusão.

Não esqueça de documentar muito bem todas essas justificativas e definições, pois os/as titulares de dados têm direito de acessá-las. Esse material também servirá de base para o passo seguinte, quando as decisões serão sistematizadas em políticas.

Também é muito importante organizar os dados em documentos com acesso restrito às pessoas que precisam trabalhar com eles, para evitar vazamentos. Lembre-se de considerar a especificidade de proteção dos dados sensíveis. Além de restringir ainda mais o acesso ou o tempo de armazenamento deles, você pode elaborar um termo de confidencialidade para colaboradores/as e voluntários/as que trabalhem com essas informações.

6° PASSO: REDIGIR OS DOCUMENTOS DE PROTEÇÃO DE DADOS

Agora é hora de criar - ou ajustar, caso já existam - os documentos que comprovam que sua organização está adequada ao que a LGPD estabelece.

Vamos ver quais são os documentos necessários?

- **Política de Privacidade**
- **Aviso de Cookies (rastreadores)**
- **Política Interna de Proteção de Dados**
- **Política de Proteção de dados pessoais de colaboradores/as**
- **Política de Segurança da Informação**
- **Política de Incidente de Insegurança**

Política de Privacidade
Deve estar acessível para os/as titulares de dados e deve conter:

- quem é o/a encarregado/a de dados da instituição e como entrar em contato;
- como se dá a captação de cada tipo de dado pessoal;

- qual a finalidade da captação de cada tipo de dado pessoal;
- quais os mecanismos de proteção das informações captadas;
- quais os programas e *softwares* utilizados para tratar as informações;
- quais são os/as operadores/as envolvidos/as no tratamento de dados da sua instituição;
- se há ou não compartilhamento de dados, se é realizado com terceiros/as de dentro ou de fora do país e qual sua finalidade;
- qual o período de armazenamento e a maneira de descarte das informações captadas.

Aviso de *Cookies* (rastreadores)
Você precisará entender, junto a profissionais de Tecnologia da Informação, se o site da sua instituição faz uso de rastreadores para acessar as preferências dos/as visitantes, como, por exemplo, qual a área do site mais acessada. Em caso afirmativo, crie um texto simples que informe que o site utiliza *cookies*, o que é rastreado e qual a finalidade do rastreamento.

Dessa forma, sua organização estará cumprindo a exigência mínima da LGPD. O ideal é que, quando possível, você invista em tecnologias que permitam ao/à titular de dados desativar *cookies* para poder acessar seu site sem ser rastreado/a.

Política Interna de Proteção de Dados
Esse documento serve para apresentar, à sua equipe, os instrumentos e fluxos que foram definidos para captação e tratamento de dados pessoais na sua instituição. É importante que ele contenha: a finalidade e a justificativa legal para cada tipo de informação coletada; as regras de compartilhamento e exclusão de dados; as funções básicas e os contatos do/a encarregado/a; e todos os conceitos que serão utilizados neste e nos demais documentos relacionados à LGPD.

Lembre-se que essa Política será a referência para seus/suas colaboradores/as e voluntários/as na hora de lidar com dados pessoais! Então,

não deixe de registrar tudo que qualquer profissional da organização precisa saber para garantir a aplicação da LGPD. Por exemplo: critérios para identificação de dados sensíveis; recomendações de anonimização; e regras para compartilhamento de informações com instituições parceiras, jornalistas, fornecedores/as, etc.

No caso de captação ou tratamento de dados realizado no âmbito de parcerias, considere a elaboração de termos coletivos de responsabilidade com a privacidade das pessoas que cedem seus dados para esse grupo ou parceria.

Política de Proteção de dados pessoais de colaboradores/as
Serve para informar o interesse da instituição na captação de dados pessoais de colaboradores/as, no momento da contratação, expondo as justificativas legais para isso, geralmente ligadas à legislação trabalhista.

A Política de Proteção de dados pessoais de colaboradores/as deve conter:

- os tipos de dados coletados em processos seletivos e na hora da contratação;
- eventuais diferenças existentes entre contratação de profissionais *freelancers* e efetivos/as;
- diferenciação entre dados tratados por obrigação legal e por legítimo interesse do/a controlador/a, por exemplo para implementar políticas de inclusão e diversidade na sua equipe;
- explicação sobre os serviços de monitoramento das atividades dos/as funcionários/as e da organização, como ponto biométrico e câmeras de vídeo;
- explicação de como se dá o monitoramento da navegação na internet e uso do telefone, se houver;
- apresentação dos direitos dos/as funcionários/as em relação aos seus dados;
- o período de retenção dos dados coletados na contratação;

- apresentação das situações em que os dados obtidos na contratação podem ser compartilhados, com quem e por quais razões.

Política de Segurança da Informação

Essa política irá orientar sua equipe ou terceirizados/as sobre as condutas adequadas para proteger a confidencialidade, a integridade e a disponibilidade dos dados coletados e armazenados pela organização, enfatizando a responsabilidade de cada um/a por esse cuidado.

Esse documento irá consolidar a estrutura de proteção de dados da instituição, pode ser solicitado pela Autoridade Nacional de Proteção de Dados (ANPD) e serve como atenuador da responsabilidade do/a controlador/a, em caso de um incidente de segurança da informação. Para elaborá-lo, será preciso uma interlocução com profissionais de Tecnologia da Informação (TI), pois é preciso expor o funcionamento dos mecanismos virtuais de proteção, armazenamento e tratamento das informações.

Basicamente, uma Política de Segurança da Informação deve conter:

- principais conceitos relacionados à Segurança da Informação;
- classificação de cada tipo de informação em níveis de confidencialidade;
- quais são os provedores de armazenamento e proteção dos arquivos da instituição;
- quais as recomendações dadas aos/às funcionários/as sobre o uso de computadores e internet dentro da empresa, o acesso a arquivos ou *download* de programas ou conteúdos;
- apresentação do/a responsável de TI da instituição, seja um/a profissional da sua equipe ou terceirizado/a.

Política de Incidente de Insegurança

Atenção, esse documento é muito importante! Ele vai balizar a atuação do/a encarregado/a de dados e da própria instituição, caso aconteça um incidente de proteção de dados. Ressaltamos que incidentes podem ocorrer, mesmo

com todas as medidas de adequação à Lei. O importante é que você tenha se precavido antes e reaja da melhor forma - isso pode atenuar eventuais penalidades por danos provocados a titulares de dados.

Seu maior objetivo é definir as tarefas de cada pessoa diante de um incidente de segurança, por isso, deve trazer os procedimentos a serem adotados em caso de comprometimento ou violação de dados pessoais, como acessos não autorizados, perdas ou roubos de um sistema de informações.

A Política de Incidente de Insegurança deve conter:

- definição sobre o que é um incidente de segurança;
- definição de quem vai formar a equipe de resposta a esse incidente ou de quem ficará responsável para lidar com o incidente junto ao/à encarregado/a;
- apresentação de áreas de suporte nessas situações: jurídico, TI e encarregado/a de dados;
- indicação de como colaboradores/as devem proceder ao perceber a falha;
- indicação de como a equipe de resposta deve avaliar a gravidade do incidente;
- apresentação de exemplos de incidentes, como dados que foram compartilhados sem uma justificativa legal, e também de situações em que dados foram devidamente protegidos pela instituição.

Para avaliar a gravidade de um incidente, sugerimos a utilização de uma matriz de risco e de uma matriz de severidade.

A matriz de risco, a ser criada de acordo com o contexto da sua organização, pode ser usada para classificar o incidente, transformando, em uma pontuação, o que pode ser considerado um risco para a proteção de dados.

Confira abaixo o exemplo da matriz de risco que usamos no Idec:

Variável	Ocorrência	Fator de multiplicação	Pontuação
Quantidade de dados	Quantidade pequena de dados (até 750 pessoas)	1 x 15	15
	Quantidade média (entre 750 e 1750 pessoas)	2 x 15	30
	Quantidade alta (mais de 1750 pessoas)	3 x 15	45
Tipo de dado	Dados pessoais não sensíveis e não financeiros	1 x 15	15
	Dados pessoais não sensíveis e financeiros	2 x 15	30
	Dados pessoais sensíveis (raça, gênero, saúde)	3 x 15	45
Caráter político	Incidente não relacionado com qualquer ocorrência política	1 x 15	15
	Incidente provavelmente relacionado com ocorrência política	2 x 15	30
	Incidente diretamente ligado com ocorrência política	3 x 15	45

Você pode ver que, no nosso caso, identificamos o risco de ataques relacionados à aparição pública do Idec em campanhas com alto teor político. Isso demonstra como o processo de adequação deve ser customizado para cada contexto, pois apenas algumas instituições se encaixam nesse caso.

Com a matriz de risco, você atribui uma pontuação específica para cada tipo de ocorrência. Somando todos os pontos, é possível, então, classificar um incidente como menos ou mais grave, a partir de uma matriz de severidade. A nossa ficou assim:

Matriz de severidade	
Baixa menos grave	Até 45 pontos
Média	Entre 45 pontos e 75 pontos
Alta mais grave	Acima de 75 pontos

Essa classificação é fundamental para que você identifique incidentes com maior potencial de dano aos/às titulares de dados e à sociedade. Incidentes graves devem ser comunicados às pessoas envolvidas. Nesse caso, pense em uma comunicação simples e eficiente, que não gere pânico e demonstre que medidas foram ou serão adotadas. O mesmo vale para a ANPD, que deve ser informada sobre incidentes com potencial risco para a sociedade.

Os demais tipos de incidente, que não causam dano ou repercussão grave, devem apenas ser registrados internamente na organização, por meio de um formulário padrão, por exemplo.

7º PASSO: DEFINIR O/A ENCARREGADO/A DE DADOS

Depois dessa jornada envolvendo todas as pessoas da sua equipe, ou pelo menos todas as que lidam com dados, você estará em condições de definir quem será o/a encarregado/a de dados (*Data Protection Officer - DPO)* da instituição. Lembrando que essa pessoa será responsável pelas atividades de tratamento de dados pessoais e pelo contato com a Autoridade Nacional de Proteção de Dados (ANPD) e com os/as titulares. Você também pode optar por contratar uma empresa para essa função.

O/a encarregado/a não precisa ser advogado/a ou profissional da área da tecnologia, mas precisa entender bem os conceitos da Lei e os fluxos de dados da instituição, sendo capaz de operar seus mecanismos de proteção de dados. É interessante que seja alguém que participou do processo de adequação e tenha bastante jogo de cintura para se relacionar com o público, atendendo suas demandas e trazendo, para a instituição, sugestões de melhorias, quando necessário.

As principais funções desse/a profissional ou empresa são:

- aceitar reclamações e comunicações dos/as titulares de dados e encaminhar suas demandas;

- receber comunicações da ANPD e adotar as providências cabíveis; e

- orientar colaboradores/as e parceiros/as da instituição sobre conceitos e práticas que garantem a proteção de dados pessoais.

Conheça, a seguir, as tarefas que o/a encarregado/a de proteção de dados deve estar apto/a a realizar:

- Monitorar o funcionamento da estrutura de proteção de dados criada a partir da adequação à LGPD, por meio da identificação e análise das atividades de coleta e tratamento de dados, para garantir que o que foi estabelecido está sendo cumprido, informar eventuais questões e fazer recomendações para o/a controlador/a;

- Manter atualizado o mapeamento dos fluxos de dados dentro da instituição e comunicar internamente, à ANPD e aos/às titulares de dados, eventuais mudanças na captação e tratamento de dados, sempre com base nas justificativas previstas na Lei;

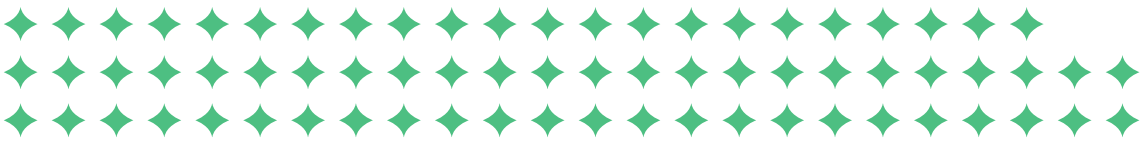
- Produzir Relatórios de Impacto à Proteção de Dados Pessoais (RIPD). Esse documento deve ser solicitado pela organização ao/à encarregado/a sempre que houver dúvida se uma determinada atividade pode colocar em risco direitos fundamentais e liberdades civis dos/as titulares de dados. Ele deve conter uma análise da situação à luz da LGPD e, caso o/a controlador/a não siga suas recomendações, deverá justificar essa decisão por escrito;

- Ser um ponto de contato da sua organização com a ANPD, atendendo suas demandas ou esclarecendo eventuais dúvidas quanto à aplicação da LGPD;

- Responder às solicitações de informação e questionamentos feitos por titulares a respeito dos mecanismos de proteção dos dados pessoais confiados à sua organização;

- Identificar pontos críticos dos processos que envolvem dados e trabalhar para repará-los;

- Realizar acordos de processamento de dados com terceiros/as com os/as quais os bancos de dados da instituição sejam compartilhados total ou parcialmente.



CHECKLIST

Estamos chegando ao final deste Manual e esperamos que você esteja bem informado/a sobre a LGPD, consciente da importância dessa Lei para a privacidade e proteção de dados pessoais e preparado/a para iniciar e/ou dar continuidade à adequação de sua instituição.

Compartilhamos esse *checklist** para conferir se realizou as principais ações necessárias para um processo eficaz de implementação da legislação em sua organização:

- [ ] Engajamento da gestão da sua organização no processo de adequação à LGPD, garantindo os recursos humanos e financeiros necessários.

- [ ] Definição do objetivo, ou seja, do foco específico e estratégico da sua organização, que vai guiar o processo de adequação à LGPD.

- [ ] Conscientização de colaboradores/as e parceiros/as sobre a Lei e criação de um programa permanente de capacitação sobre o tema.

  Uma dica: este manual pode ser usado como material de apoio nesse processo, pois traz os principais conceitos e determinações da Lei, em linguagem acessível!

- [ ] Identificação e engajamento de colaboradores/as e gestores/as que se envolverão diretamente nos processos de adequação.

- [ ] Identificação e contato com agentes externos relevantes, como outras organizações que tenham perfil parecido com a sua e/ou experiências interessantes com a LGPD.

- [ ] Contratação de especialistas para dar consultoria para sua equipe ou executar etapas mais técnicas do processo de adequação.

* Inspirado no checklist produzido pelo Centre Dor Information Policy Leadership (CIPL) em Parceria com o Centro de Direito Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS – IDP). https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[pt]_cipl-idp_white_paper_on_top_priorities_for_organizations_to__effectively_implement_the_lgpd_7_october_2020_.pdf

- [ ] Mapeamento de todos os dados pessoais coletados e armazenados e de todas as atividades de tratamento realizadas por sua organização, com a identificação de:
  - meios de coleta e armazenamento de dados;
  - dados pessoais sensíveis tratados;
  - finalidade do tratamento;
  - terceiros que realizem tratamento de dados pessoais em nome da sua organização;
  - casos em que sua instituição trata informações em nome de terceiros, se houver;
  - terceiros com os quais sua organização compartilha dados pessoais;
  - fluxos internacionais de entrada e saída de dados da instituição.

- [ ] Avaliação dos riscos relacionados ao tratamento de dados pessoais realizado por sua organização, incluindo riscos para titulares dos dados.

- [ ] Eliminação de captações e tratamentos de dados desnecessários.

- [ ] Determinação das bases legais que justificam as captações e tratamentos de dados.

- [ ] Anonimização dos dados que puderem ser utilizados sem a identificação de titulares.

- [ ] Definição do tempo de armazenamento e da forma de eliminação para cada tipo de dado pessoal tratado.

- [ ] Atualização de contratos para refletir e regulamentar o papel da sua organização (como controladora ou operadora) em relação a terceiros.

- [ ] Criação de avisos e inclusão de cláusulas em documentos para informar titulares, de forma clara e acessível, sobre os dados coletados, os tratamentos e suas finalidades.

- [ ] Elaboração de documentos que consolidam sua política de proteção de dados pessoais: Política de Privacidade, Aviso de *Cookies* (rastreadores), Política Interna de Proteção de Dados, Política de Proteção de dados pessoais de colaboradores/as, Política de Segurança da Informação, Política de Incidente de Insegurança.

- [ ] Identificação e implementação dos mecanismos de transferência internacional de dados mais apropriados para sua instituição, se for o caso.

- [ ] Implementação de medidas de segurança técnicas e administrativas para proteger os dados pessoais e garantir o gerenciamento de possíveis incidentes de segurança.

- [ ] Definição de encarregado/a de dados, documentação e comunicação interna sobre seu papel e suas responsabilidades.

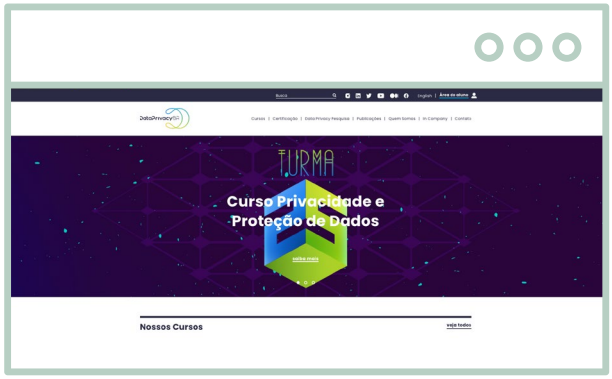
- [ ] Desenvolvimento de processos eficientes para responder as solicitações de titulares de dados dentro do prazo estabelecido na legislação, a partir de um levantamento das possíveis solicitações.

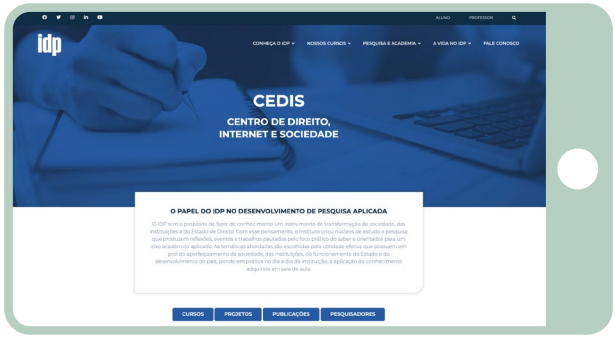
- [ ] Estabelecimento de processo interno de notificação e de gerenciamento de incidentes de segurança e de vazamento de dados, que considere comunicação à ANPD e aos/às titulares quando necessário.

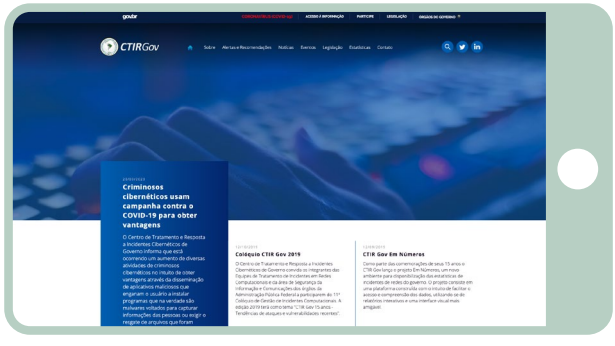
- [ ] Manutenção e revisão contínua dos processos de adequação à LGPD.

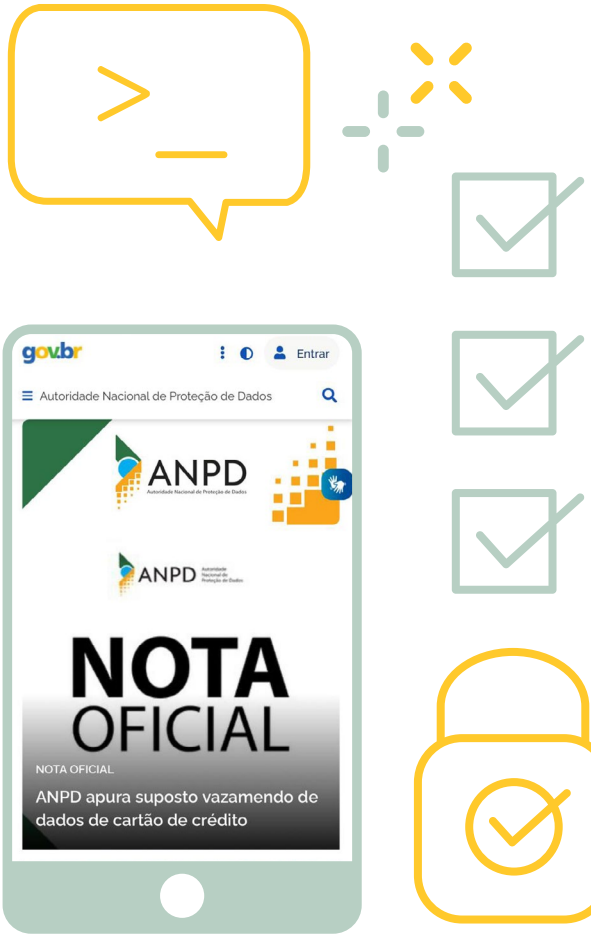
REFERÊNCIAS IMPORTANTES

Para saber mais sobre proteção de dados pessoais e se atualizar sobre a LGPD

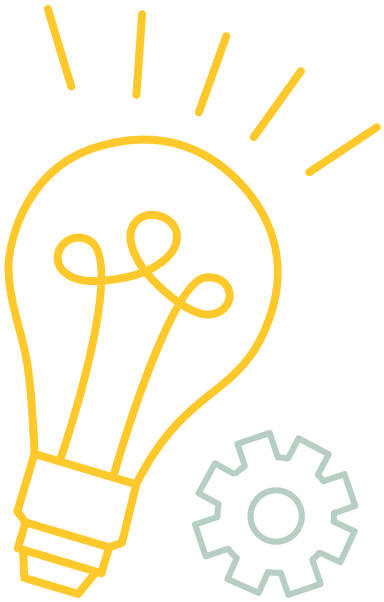


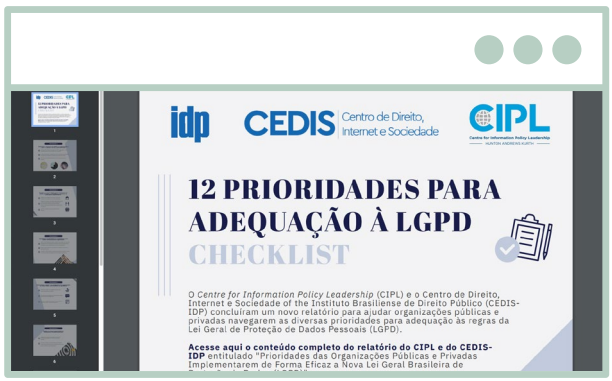


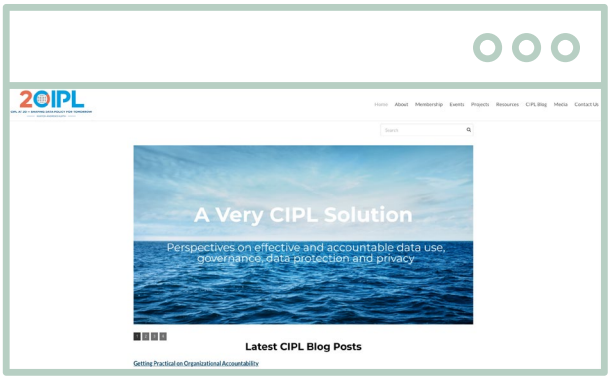




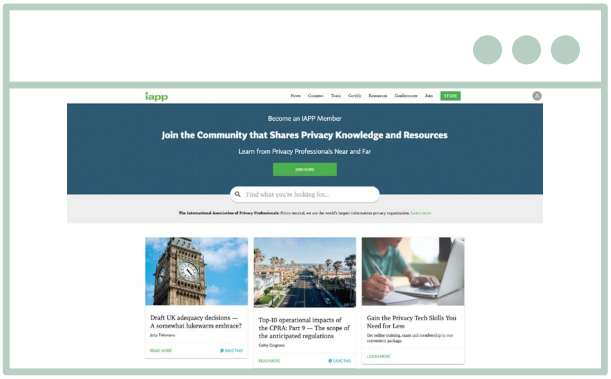

Observatório
Sobre Blog Boletim Memória Contato
Memória da LGPD
Para contar e explicar o longo processo de construção e aprovação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), o Observatório da Privacidade e Proteção de Dados, projeto do Data Privacy Brasil, entrevistou 18 pessoas que tiveram participação fundamental na história. Confira!
ver episódios
Observatório da privacidade e proteção
O Observatório é uma plataforma de monitoramento, resgate e análise sobre os debates em torno do tema da privacidade e proteção de dados pessoais no Brasil.




idp
CEDIS Centro de Direito, Internet e Sociedade
CIPL
12 PRIORIDADES PARA ADEQUAÇÃO À LGPD
CHECKLIST
O Centre for Information Policy Leadership (CIPL) e o Centro de Direito, Internet e Sociedade of the Instituto Brasiliense de Direito Público (CEDIS-IDP) concluíram um novo relatório para ajudar organizações públicas e privadas navegarem as diversas prioridades para adequação às regras da Lei Geral de Proteção de Dados Pessoais (LGPD).
Acesse aqui o conteúdo completo do relatório do CIPL e do CEDIS-IDP entitulado "Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de


2 CIPL
A Very CIPL Solution
Perspectives on effective and accountable data use, governance, data protection and privacy
Latest CIPL Blog Posts
Getting Practical on Organizational Accountability


ico.
Guide to the UK General Data Protection Regulation (UK GDPR)


iapp
Become an IAPP Member
Join the Community that Shares Privacy Knowledge and Resources
Learn from Privacy Professionals Near and Far
Draft UK adequacy decisions — A nonevolutionary embrace?
Top-10 operational impacts of the CPRA: Part 9 — The scope of the anticipated regulations
Gain the Privacy Tech Skills You Need for Less

Glossário

AGENTES DE TRATAMENTO DE DADOS: abrange os termos “controlador/a” e “operador/a” de dados. Quando usado no singular (“Agente”), se refere a um dos dois termos.

ANONIMIZAÇÃO: procedimento por meio do qual a ligação entre o/a titular de dados e suas informações é quebrada, impedindo sua identificação a partir dos dados retidos por uma instituição.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): órgão da administração pública federal, integrante da Presidência da República. Suas tarefas essenciais são fiscalizar e regular a aplicação da LGPD e a ideia é que a entidade, enquanto representante do interesse público, faça a ponte entre a sociedade e o governo. A ANPD também terá o papel de orientar e apoiar outros órgãos do governo, OSCs e empresas em relação ao tratamento de dados.

BANCO DE DADOS: conjunto estruturado de dados pessoais ou anonimizados, localizado em um ou em vários locais, em suporte eletrônico ou físico.

COMPARTILHAMENTO DE DADOS: comunicação, difusão, transferência internacional ou tratamento compartilhado de bancos de dados pessoais, com autorização específica, entre entes públicos ou privados.

CONSENTIMENTO: autorização livre e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

CONTROLADOR/A DE DADOS: pessoa física ou jurídica que pode ser identificada como responsável pelas decisões sobre a finalidade do tratamento de dados, o meio de captação e os fluxos envolvendo tais informações.

***COOKIES* (RASTREADORES):** arquivos enviados por servidores de sites e plataformas para o computador ou celular de usuários/as com a finalidade de identificar o computador ou celular e obter dados de acesso, que são considerados dados pessoais. Esses dados permitem identificar o perfil de usuários/as e podem ser usados para garantir uma maior segurança e personalizar sua experiência nos sites e plataformas.

DADOS MANIFESTAMENTE PÚBLICOS: informações que podem ser utilizadas livremente porque estão disponíveis nos portais de autoridades governamentais, como a Receita Federal, Portais da Transparência e os diversos Tribunais de Justiça.

DADOS PESSOAIS: todos e quaisquer dados que possibilitem a identificação de alguém, por exemplo: telefone, endereço, CPF, endereço I.P., link de perfil em redes sociais, etc.

DADOS PESSOAIS ANONIMIZADOS: dados pessoais que passaram por um processo de anonimização e que não podem ser associados a nenhum indivíduo específico.

DADOS PESSOAIS SENSÍVEIS: informações sobre aspectos da vida de alguém que podem gerar situações delicadas, como algum tipo de discriminação ou exposição. A partir da Lei, consideram-se sensíveis os seguintes dados: orientação sexual; orientação religiosa; filiação política ou partidária; raça; dados de saúde, genéticos e biométricos.

ELIMINAÇÃO: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independente do procedimento empregado.

ENCARREGADO/A: pessoa, nomeada pelo/a controlador/a, responsável pelas atividades de tratamento de dados pessoais da instituição e pelo contato com a Autoridade Nacional de Proteção de Dados (ANPD) e com titulares de dados, atendendo suas demandas. Também conhecido/a como encarregado/a de proteção de dados ou DPO (*Data Protection Officer*).

FINALIDADE: propósito legítimo, baseado na lei e informado ao/à titular, que assegura a legalidade do tratamento de seus dados.

INCIDENTE DE INSEGURANÇA: violação de segurança que provoca, de modo acidental e ilícito, a destruição, a perda, a alteração, a divulgação de dados ou o acesso não autorizado a dados pessoais sujeitos a qualquer tipo de tratamento.

OPERADOR/A DE DADOS: pessoa física ou jurídica que realiza o tratamento de dados a mando do/a controlador/a, segundo suas diretrizes.

TRATAMENTO DE DADOS: todo procedimento realizado com dados pessoais, desde o momento em que a informação entra em um banco de dados até ser excluída dele. Por exemplo: coletar, armazenar, transferir, formular, analisar, inserir em planilhas, realizar monitoramento ou publicidade a partir das informações, compartilhar com terceiros/as, etc.

Expediente

Coordenação executiva: Teresa Liporace

Pesquisa e redação: Maraísa Rosa e Rafael Zanatta

Supervisão técnica: Bárbara Prado Simão e Diogo Moyses

Produção editorial: Dayse Porto

Edição e revisão de texto: Angela Roman e Raquel Porangaba

Projeto gráfico e diagramação: Renata Fagundes

Agradecimentos: Livia Linhares, Victor Amorim e Mariana Toledo, pela participação no grupo focal realizado para o desenvolvimento deste conteúdo, Mariana Rielli, Iasmine Favaro e Thais Aguiar, pelos comentários sobre o material.

Realização: idec Instituto Brasileiro de Defesa do Consumidor

Apoio: FORD FOUNDATION OPEN SOCIETY FOUNDATIONS

Somos uma organização da sociedade civil sem fins lucrativos que atua para proteger e ampliar os direitos dos/as consumidores/as, de forma independente de governos, partidos políticos e empresas. Nosso trabalho é mantido com recursos de projetos de fundações filantrópicas e por doações de pessoas físicas que acreditam na importância do que fazemos.

Desde 1987, representamos consumidores/as de todo o país na luta por relações de consumo mais justas, especialmente nas áreas de **telecomunicações e direitos digitais**, serviços financeiros, saúde, alimentação saudável, mobilidade urbana, e energia. Na luta pelos direitos digitais, nossa organização foi protagonista no processo de elaboração e aprovação da Lei Geral de Proteção de Dados e, desde sua aprovação, nos comprometemos com a educação e conscientização da sociedade brasileira em relação a dados pessoais.