Carta Técnica

LGPD na prática

Manual de boas práticas e principais conceitos sobre a Lei Geral de Proteção de Dados Pessoais para entidades do terceiro setor

FUNDAÇÃO FEAC

1. O que é a LGPD?

Em uma época em que o alcance das nossas informações aumentou muito por causa das ferramentas digitais, tornou-se importante também aumentar a proteção às informações de cada um de nós, que também chamamos de dados pessoais. A LGPD ou Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) entrou em vigor em 18 de setembro de 2020 e cria novas obrigações para proteção de dados pessoais, sejam eles digitais ou não, estabelecendo mais direitos aos indivíduos e mais obrigações às organizações públicas ou privadas que usam dados pessoais no Brasil.

Além disso, cria regras claras sobre os processos de coleta, armazenamento e compartilhamento dessas informações para que não sejam usadas de maneira errada ou diferente do que foi informado para o titular.

Isso ajuda a promover o desenvolvimento tecnológico ao mesmo tempo que procura garantir a segurança dos indivíduos. Com essa lei, o Brasil passou a integrar um grupo de 134 países que implementam leis de proteção de dados no mundo.

2. Personagens e termos da lei

A LGPD traz nomes e conceitos novos do âmbito jurídico, mas é importante conhecê-los.
Vamos dar uma olhada neles?

• **Titular** – Pessoa física que é a proprietária dos dados pessoais. Todos nós somos titulares de dados e os compartilhamos diariamente com empresas, entidades e o Poder Público.

• **Controlador** – A pessoa física ou jurídica que decide a respeito do tratamento dos dados pessoais. Exemplo: uma empresa que coleta dados para empregar funcionários, uma escola que coleta dados de alunos.

• **Bases legais** – Uma base legal é uma finalidade prevista em lei para que empresas, entidades e o poder público possam tratar dados pessoais. Exemplo: a execução de um contrato de trabalho é uma finalidade prevista para coletar dados necessários de funcionários. O consentimento pode ser uma base legal para mandar e-mail marketing. O cumprimento de obrigação legal pode requerer que você guarde alguns dados coletados por um período de tempo. Existem 10 bases legais dando permissões diferentes para o uso de dados pessoais.

• **Tratamento** – É qualquer tipo de operação realizada com o uso de dados pessoais. Alguns exemplos são a coleta, acesso, armazenamento, distribuição, avaliação, modificação, processamento, transferência recepção e mesmo a eliminação desses dados.

• **Dado anonimizado** – É o dado relativo a um titular que não pode ser mais identificado, considerando a utilização de meios técnicos razoáveis na ocasião de seu tratamento. Exemplo: quando, em uma pesquisa, apenas dados genéricos são coletados que identifiquem a pessoa a um grupo (homem, 60 anos, aposentado) e não tenha capacidade de identificá-lo individualmente. No entanto, se houver qualquer dado que identifique a pessoa (endereço, por exemplo), ele deixa de ser anonimizado.

• **Encarregado** – Responsável da instituição, para acompanhar o tratamento de dados dos titulares, e ser o canal de comunicação com titulares, Autoridade Nacional e parceiros. Pode ser pessoa física ou jurídica.

• **Operador** – Pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador. Exemplo: uma assessoria contábil que processa pagamentos de funcionários de várias empresas, uma solução em nuvem que hospeda dados.

• **Dados pessoais** – É a informação relacionada a uma pessoa identificada ou identificável. Ele pode ser o seu CPF isoladamente, o seu endereço, um login de e-mail ou mesmo uma foto, que pode ser reconhecida em um aplicativo que vai relacionar esta foto a você.

• **Dados pessoais sensíveis** – 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. Têm hipóteses mais restritas de tratamento.

3. Encarregado versus empresa de pequeno porte e OSC

A ANPD apresentou em 2022 a Resolução nº 2, de 27 de janeiro de 2022, direcionada para microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos. Essa resolução desobriga os agentes de pequeno porte de indicar um encarregado/DPO (data protection officer). Mesmo com essa desobrigação, as OSC têm a necessidade de disponibilizar um canal de comunicação com o titular de dados. Além disso, é obrigatório adotar medidas de segurança da informação.

Outro ponto importante é o prazo dobrado para atendimentos de solicitações dos titulares de dados, porém o prazo segue em 15 dias para fornecimento ao titular de dados de declaração simplificada de quais dados a entidade trata.

Não poderão se beneficiar desta resolução os agentes de tratamento de pequeno porte que realizem tratamento de alto risco para os titulares. O que pode ser considerado alto risco? Quando, entre outras questões, essas duas situações ocorrerem conjuntamente: I. tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares; II. utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

4.Como tratar dados pessoais

Nós usamos dados pessoais para tudo. Damos nosso CPF para comprar produtos, fazemos login para acessar nosso e-mail, registramos pessoas em fotos, que depois são marcadas por ferramentas de reconhecimento facial, que as identifica.

Mas, com a chegada da LGPD, existem regras para o que podemos ou não fazer com os dados pessoais dos outros, como empresa, entidade ou Poder Público. Vamos ver aqui um pouquinho do que são e como usar as bases legais que mencionamos e outros requisitos especiais, como o tratamento de dados pessoais de menores.

Consentimento – Autorização para tratamento de dados. As informações sobre o tratamento devem ser claras e acessíveis. O uso deve ser específico apenas para aquela finalidade solicitada. O consentimento deve ser registrado. Lembre-se de que o consentimento não é a única forma de usar dados pessoais. Existem também as opções a seguir.

Execução de contrato – Quando os dados são necessários para que um contrato possa ser assinado. Exemplo: verificação da situação cadastral de um fornecedor junto à Receita Federal, endereço de entrega de itens adquiridos pela internet, contratação de funcionário.

Cumprimento de obrigação legal – Quando uma lei obriga que dados pessoais sejam guardados por certo período de tempo, a entidade deve cumprir o que pede a lei e guardar os dados pelo tempo necessário (exemplo: dados de ex-funcionários, colaboradores, ex-alunos, dados médicos em entidades que trabalhem na área da saúde).

Exercício regular de direito – O exercício regular de direitos permite o uso de dados pessoais em contrato e em processo judicial, administrativo e arbitral. Por exemplo, para apresentar um documento em juízo, para fazer prova em processo judicial, mesmo apresentando dados sensíveis, como dados de saúde.

Proteção da vida – A proteção da vida tem escopo de aplicação mais limitado. Seu uso pode ser levantado durante o monitoramento de epidemias, para garantir ajuda humanitária, para tratar paciente inconsciente, para internação de urgência ou campanhas de vacinação em empresas ou instituições.

Tutela da saúde – O tratamento de dados com base na tutela da saúde é aplicável exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Esses dados também não podem ser compartilhados para obter vantagem econômica.

Execução de políticas públicas – Dados pessoais também poderão ser usados para a execução de políticas públicas, para o atendimento de necessidades e solução de problemas da coletividade. Exemplo: cadastro de bolsa família, auxílios emergenciais e política de cotas.

Estudo por órgão de pesquisa – Os estudos por órgãos de pesquisa têm um papel importante no desenvolvimento econômico. São órgãos da administração pública direta ou indireta, sem finalidade lucrativa. Assim, órgãos de pesquisa privada não podem se valer dessa finalidade para uso indiscriminado de dados.

Proteção ao crédito – A base de proteção ao crédito pode ser usada para a criação de cadastros de inadimplentes e também de adimplentes (cadastro positivo) para avaliação de risco de crédito, quando o titular solicita um empréstimo, financiamento ou vai contratar determinados serviços.

Interesse legítimo do controlador ou terceiros – Quando alguém já tem um relacionamento anterior com uma instituição, seja como doador, voluntário ou colaborador, entende-se que a instituição poderá manter essa pessoa informada de atividades, eventos, relatórios, podendo se valer do legítimo interesse sem a necessidade do consentimento para essa finalidade.

Tratamento de dados de menores de idade – O tratamento de dados pessoais de crianças deverá ser realizado com consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. As informações de tratamento devem ser dadas de forma clara e acessível. Apenas os dados estritamente necessários devem ser coletados.

Sem consentimento – Apenas em duas situações: para contatar os pais/responsáveis – sem armazenamento, sem passar para terceiros; e quando utilizado para a proteção da criança

5. Princípios da LGPD?

A LGPD tem dez princípios que precisam ser observados. E só por eles já temos uma boa ajuda do que devemos ou não devemos fazer a respeito de dados pessoais. Também temos boas dicas sobre o que você pode fazer para colocá-los em prática. Nós traduzimos aqui os 10 princípios da LGPD em perguntas que podem ajudá-lo na decisão sobre o uso dos dados:

1• Necessidade
É realmente necessário utilizar esses dados para atingir o objetivo desejado pela entidade?

2• Finalidade
Os dados estão sendo coletados para uma finalidade específica e informada ao titular?

3• Adequação
O tratamento está sendo feito de acordo com o que foi informado para o titular e não para outro fim?

4• Livre acesso
O titular pode consultar, de forma fácil e gratuita, seus dados, a forma de tratamento e sua

5• Qualidade dos dados
Os dados estão corretos, atualizados e estão de acordo com a necessidade para a finalidade?

6• Transparência
A pessoa foi informada do motivo do tratamento dos dados de forma clara e transparente?

7• Segurança
Os dados são guardados em lugar seguro, seja física, seja digitalmente?

8• Prevenção
Conseguimos prevenir da melhor maneira possível o acesso não autorizado a esses dados?

9• Não discriminação
Os dados não serão usados de maneira alguma para causar qualquer tipo de discriminação?

10• Responsabilização e prestação de contas
Somos capazes de provar que tomamos as medidas necessárias para cumprir as normas de proteção de dados?

6. LGPD na prática

Como fazer para colocar todas essas informações na prática em sua instituição? Vamos dar algumas dicas e apresentar boas práticas que podem ser adequadas à realidade de cada local.

Tratamento de dados – É preciso entender a) quais dados sua instituição coleta, b) de que forma eles são coletados e c) qual a finalidade de uso desses dados. Com isso, é possível estabelecer qual a base legal para usar esses dados e ficar de acordo com a lei. Dados que não são necessários devem ser excluídos.

Site e cadastro – Se a instituição tem um site, é importante verificar os seguintes itens: Política de Privacidade: falamos sobre ela no quadro a seguir. Cookies: se a entidade faz uso de cookies para coletar dados do usuário, é preciso notificar e pedir o aceite do usuário. Se não tem site, mas faz cadastro para qualquer finalidade, a coleta de dados para cadastro deve focar nos dados estritamente necessários e apenas para a finalidade informada.

Indicações do encarregado – O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Por enquanto, até a ANPD se manifestar a respeito das exceções, toda instituição que trata dados pessoais deve ter um Encarregado apontado. Essa pessoa pode ser indicada na Política ou Aviso de Privacidade da instituição.

Política e Avisos de Privacidade – Política de Privacidade: é necessário criar uma política de privacidade de maneira simples, informando pelo menos o seguinte: identificação e informações de contato do controlador, quais dados são coletados, com que finalidade, se esses dados são compartilhados com terceiros, quais os direitos dos titulares e como fazer para exercê-los.

Avisos de Privacidade: caso você trabalhe na sua instituição com monitoramento via câmera, monitora a internet, ou faz qualquer outro tipo de coleta de dados pessoais, é importante informar o usuário, colaborador ou visitante.

Linguagem clara e acessível – Ao explicar para o titular a finalidade do uso de dados, solicitar consentimento, quando for o caso, e explicar os direitos, é importante usar uma linguagem clara e acessível.

O uso de recursos visuais é encorajado, para facilitar o entendimento. As explicações não precisam ser em forma escrita apenas. Desenhos e gráficos podem auxiliar o entendimento.

Marketing e doações – Dentro da LGPD, alguns cuidados são muito importantes quando a entidade fizer campanhas de marketing e solicitar doações. Nunca compre listas de e-mail se não tem uma base legal para fundamentar seu uso. Não inclua contatos automaticamente sem um primeiro contato ou uma relação preexistente. Quando fizer um cadastro, não use caixas pré-marcadas obrigando o contato a receber mensagens da instituição.

Sempre solicite ao titular se ele quer receber informações da instituição. Permita que o titular possa escolher quando não quer mais receber mensagens, e-mails e ligações da instituição, incluindo um botão de descadastro no e-mail ou canais para que o titular possa fazer essa solicitação (por exemplo: um endereço de e-mail).

O titular tem direito de saber quais dados dele a instituição mantém. Ele pode solicitar a correção, alteração ou mesmo a exclusão desses dados. Forneça na Política de Privacidade da instituição um canal para que ele possa fazer essas solicitações e atenda aos pedidos feitos pelo titular.

Softwares e antivírus – Manter softwares e antivírus originais e atualizados que garantam a proteção da instituição contra malwares, ransomwares e outros ataques cibernéticos que podem colocar em risco não só os dados dos titulares, mas a segurança da organização como um todo.

Incidentes de vazamento – Caso aconteça um vazamento de dados, apesar de todos os cuidados, o controlador deverá tomar algumas medidas. Dependendo do grau do vazamento, ele deverá comunicar à Agência Nacional de Proteção de Dados e ao titular a ocorrência de um incidente de segurança.

Esse incidente pode ser uma invasão hacker com roubo de dados que possam causar dano real ao titular, por exemplo. Por isso, atenção! Em que casos isso deve ser feito? Apenas em casos que possam acarretar risco ou dano relevante aos titulares.

A comunicação deve ser feita em prazo razoável e deve conter a descrição dos dados pessoais afetados, informações sobre os titulares envolvidos, riscos, medidas adotadas. Se um incidente desses acontecer, procure imediatamente ajuda técnica e jurídica.

Revisão de contratos – Todos os contratos com fornecedores e parceiros que envolvam tratamento de dados pessoais coletados pela organização devem ser revisados e adequados à nova lei. A ausência de medidas adequadas de segurança e da adequação dos fornecedores à LGPD pode resultar em responsabilidade solidária para o controlador dos dados. Inclua no Contrato cláusulas que obriguem os parceiros a proteger os dados compartilhados.

Treinamento de equipe – O envolvimento dos colaboradores no processo garante uma melhor adequação e manutenção das boas práticas de proteção de dados como parte dos valores da entidade. O treinamento da equipe e esclarecimento com relação às boas práticas permitem que eles possam entender e participar do processo com mais clareza.

Segurança da informação – A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, sejam elas físicas, sejam digitais, evitando acessos não autorizados. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer de seu uso impróprio.

Para sua proteção, sugere-se a criação de uma Política de Segurança da Informação adequada à realidade da instituição. Aqui trazemos algumas práticas que podem ser adotadas de acordo com essa política:

Reveja a forma com que dados pessoais são armazenados, utilizando senhas em planilhas sempre que possível e mantendo os dados físicos em locais seguros, com chave.

Registre a identificação de visitantes em áreas reservadas.

Use senha nos computadores e usuários diferentes para acessos de pessoas diferentes, mesmo que utilizem o mesmo computador.

Defina quais pessoas na instituição necessitam acessar informações mais críticas.

Programe o bloqueio do computador quando não estiver em utilização.

Não deixe senhas acessíveis em post-its, embaixo do computador ou em local de fácil visibilidade.

Altere as senhas periodicamente.

Evite deixar documentos com dados pessoais expostos a quem não precisa ter acesso a eles, em especial dados sensíveis.

Descarte adequadamente os dados que não são mais necessários. Currículos devem ser triturados, mídias devem ser destruídas e backups devem ser verificados para eliminar completamente uma informação desnecessária. Dados físicos devem ser rasgados ou triturados. Não os reaproveite para fazer rascunho.

Faça uso de redes de wi-fi confiáveis.

Se possível, invista no uso de um antivírus para rastrear possíveis ameaças aos computadores da entidade.

Nos casos em que for possível, anonimize ou criptografe os dados.

Direito dos titulares – Dentro da LGPD, os titulares têm direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara e acessível indicando a) finalidade do tratamento, b) forma e duração, c) identificação do controlador e suas informações de contato, d) se os dados são compartilhados e qual a finalidade do compartilhamento, e) as responsabilidades dos agentes de tratamento e os seguintes direitos:

i. Confirmação *– Confirmação da existência de tratamento. Lembrando que tratamento pode ser qualquer ação feita com um dado pessoal: coleta, guarda, compartilhamento e mesmo a exclusão.*

ii. Acesso *– Acesso às informações que a organização tem a respeito do titular e como esses dados são tratados. A entidade tem 15 dias para responder a essa solicitação com uma cópia dos dados do titular.*

iii. Correção *– O titular tem direito de solicitar a correção dos dados que estiverem incompletos, inexatos ou desatualizados.*

iv. Eliminação *– Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei. Por exemplo: a manutenção no cadastro de um dado sensível que não é necessário para a finalidade do uso.*

v. Compartilhamento *– O titular tem direito de ser informado, quando solicitar, sobre as entidades públicas e privadas com as quais o controlador compartilhou seus dados.*

vi. Objeção *– Quando o tratamento é baseado em consentimento, o titular tem direito de saber o que acontece se ele negar consentimento. Por exemplo: não ter acesso a certas informações, como eventos, festas etc.*

vii. Retirada de consentimento *– O titular tem direito de retirar o consentimento dado quando não quiser mais receber comunicações ou contato da entidade, por exemplo. Lembre-se: isso só vale para dados tratados com base em consentimento e não com outra base.*

7. Quais as vantagens de se adequar?

Credibilidade e confiança, vantagem competitiva, evitar dano reputacional com vazamentos, evitar perda de contratos e convênios, oportunidade de aprimorar rotinas, engajamento na construção da lei.

8. Perguntas frequentes

a) Posso compartilhar dados com terceiros? Sim, é possível o compartilhamento de dados desde que exista uma finalidade adequada e legítima, assim como que o titular de dados tenha ciência do compartilhamento pretendido. Deve ressaltar que o dado coletado deve estar em conformidade com a base legal, devendo apresentar documento compatível com a base legal utilizada, como no caso de consentimento, em que deve ser criado um formulário para obtenção do consentimento específico e destacado do titular.

b) Posso vender os dados pessoais dos doadores para outras organizações? Caso a finalidade seja unicamente a comercialização dos dados pessoais, entendemos que a venda está em desconformidade com a LGPD, visto que há ausência de expectativa do titular sobre essa relação comercial e que essa ação sai do objeto da organização.

c) A organização pode ligar ou enviar e-mail para potenciais doadores? Sim, desde que observados a finalidade e os requisitos da base legal. Caso o tratamento desses dados seja baseado em legítimo interesse, deverá ser realizada uma Avaliação de Legítimo Interesse, a fim de verificar se a base legal do legítimo interesse se aplica ao seu processamento.

d) Caso solicitado, a organização deve excluir a base de dados de um doador ou beneficiário? Caso não apresente nenhuma obrigação legal ou regulatória, que obrigue a manutenção dos dados pessoais, é necessário que a organização atenda o pedido, sob pena de descumprimento da LGPD.

e) É necessário sempre pedir o consentimento do titular dos dados? Não, a LGPD apresenta 10 bases legais, sendo necessário adequar o tratamento de dados conforme cada caso. As bases legais são: consentimento, legítimo interesse, cumprimento de obrigação legal ou regulatória, exercício regular de direito, proteção da vida, tutela da saúde, execução de políticas públicas, estudo por órgão de pesquisa, proteção ao crédito e execução de contrato.

9. Links úteis

Lei Geral de Proteção de Dados Pessoais
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Glossário LGPD – Serpro
https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd

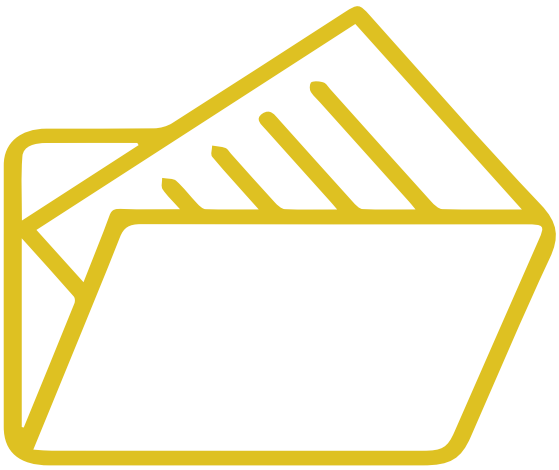
LGPD Acadêmico
Cursos, manuais e outros materiais relevantes na área de proteção de dados pessoais.
https://www.lgpdacademicooficial.com.br

Casa Hacker
A Casa Hacker fica baseada em Campinas e é um espaço hacker sem fins lucrativos e 100% dedicado a colocar comunidades locais no controle de suas experiências digitais e a moldar o futuro da tecnologia da informação e comunicação para o bem público.
https://casahacker.org

NIC.br: Núcleo de Informação e Coordenação do Ponto BR no Brasil
Tem cursos, cartilhas e pesquisas sobre segurança na internet.
https://cursoseventos.nic.br

Juventude Privada
Iniciativa socioeducativa, sem fins lucrativos, que busca promover ensinamentos sobre privacidade, proteção de dados pessoais e cidadania digital, para que os jovens estudantes possam tomar decisões informadas e se protegerem, seja na internet, seja fora dela.
https://www.juventudeprivada.org/o-projeto

Governo Digital
Guias operacionais do governo federal para adequação à LGPD.
https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd



Carta Técnica elaborada por: Paes de Mello Advocacia (PDMLaw)

Elaboração 2020: Ana Carolina Paes de Mello
Revisão 2022: Ana Carolina Paes de Mello e Beatriz Junque
Revisado por: Nathalia Garcia – Fundação FEAC

Os produtos de conhecimento FEAC estão em constante aprimoramento. Colabore enviando sugestões e considerações. Todas as contribuições são bem-vindas.

www.feac.org.br

FUNDAÇÃO FEAC