Boas práticas de proteção de dados (LGPD) para o terceiro setor

Casa Hacker

INSTITUTO PRO BONO

KLA

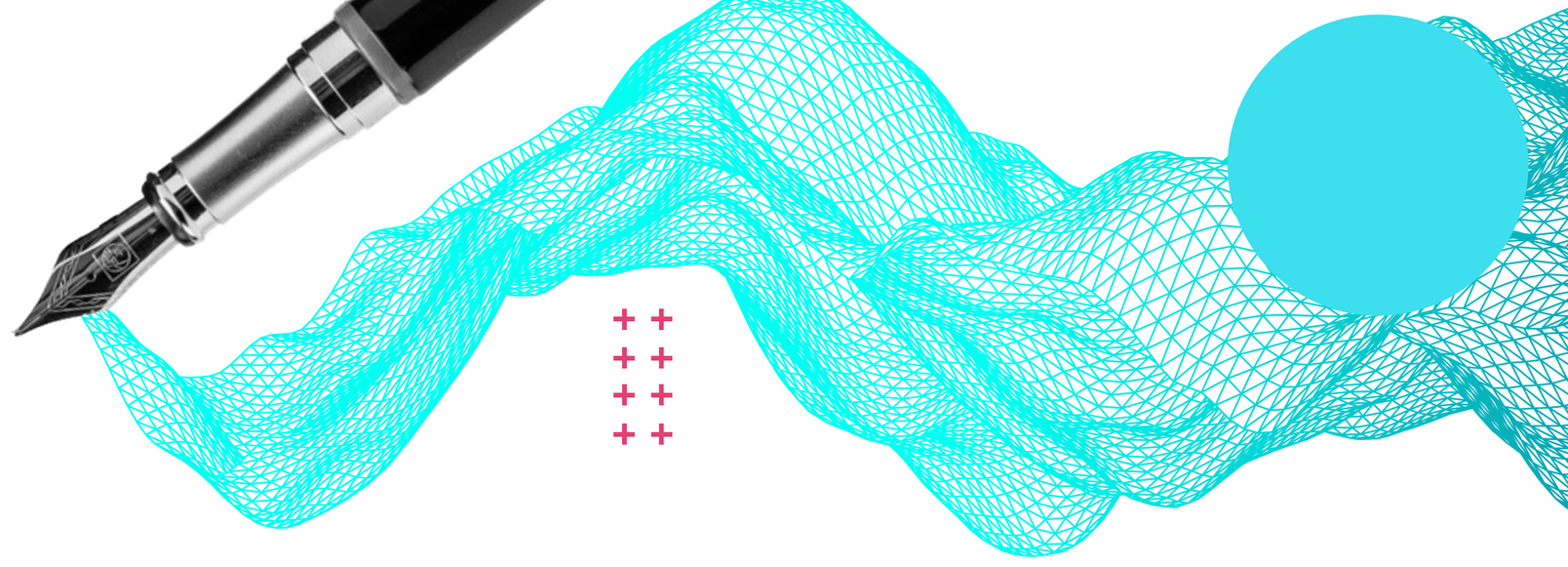
A cartilha a seguir é resultado da colaboração entre Instituto Pro Bono, Casa Hacker e Koury Lopes Advogados (KLA). A conexão entre as três instituições já possui uma história. Ano passado, a Casa Hacker buscou o Instituto Pro Bono para receber atendimento jurídico gratuito para formalizar-se enquanto organização da sociedade civil e receber a orientação jurídica sobre compliance, captação de recursos e política de dados. Assim, o KLA, escritório voluntário do Instituto Pro Bono, prontificou-se a atendê-la de forma voluntária.

O atendimento jurídico pro bono possibilitou uma colaboração entre as partes em uma temática congruente: a proteção de dados em organizações do terceiro setor. Dessa forma, Instituto Pro Bono, Casa Hacker e KLA reuniram-se para produzir um material específico de boas práticas sobre este assunto. O objetivo deste material é guiar gestores e comunicadores do terceiro setor sobre proteção de dados e também a recente Lei Geral de Proteção de Dados.

Para melhorar a leitura, sugerimos atentar-se ao Glossário.

Boa leitura!

ÍNDICE



COLETA

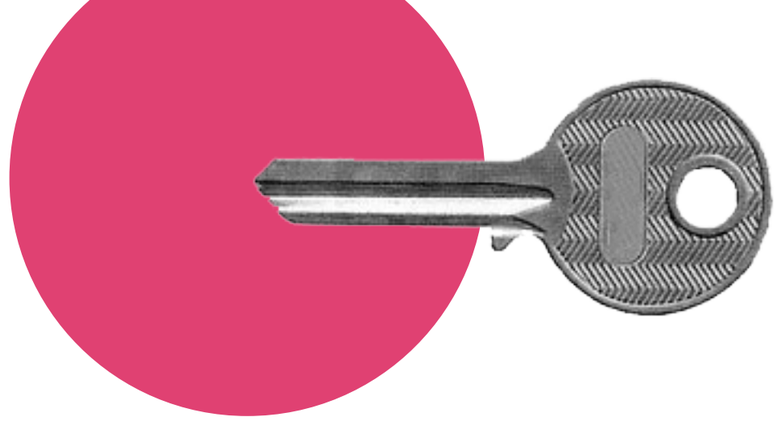
Como posso coletar os Dados Pessoais de visitantes em meu site?

É possível coletar Dados Pessoais por meio de formulários, cookies, tags, IP's, entre diversas outras ferramentas. Porém, as finalidades das coletas devem estar amparadas pelas bases legais da LGPD e os Titulares dos Dados devem ser informados sobre quais de seus Dados Pessoais estão sendo coletados e para quais finalidades (essas informações podem ser indicadas por meio de uma política de privacidade, por exemplo).

Dica

A elaboração de uma **política de privacidade** indicando as atividades de coleta de Dados Pessoais de forma clara e transparente, permitindo ao visitante (Titular) não aceitar a coleta de determinados Dados Pessoais não essenciais para o funcionamento do site, é de suma importância no respeito dos direitos do Titular estabelecidos na LGPD, bem como aos princípios da própria LGPD e do Marco Civil da Internet.

USO E ACESSO



Quem pode ter acesso a Dados Pessoais?

Somente os profissionais que tenham necessidade de ter acesso e Tratar esses Dados Pessoais para a finalidade para os quais eles foram coletados deveriam ter acesso a tais informações.

Dica

A restrição de acesso aos Dados Pessoais baseada nos princípios *need-to-know* e *least privilege* é considerada uma boa prática no Tratamento de Dados Pessoais. O acesso ilimitado aos Dados Pessoais coletados não só potencializa riscos de vazamentos, como também desvirtua a finalidade original de sua coleta.

Como posso utilizar esses Dados Pessoais?

Os Dados Pessoais podem ser usados livremente desde que exista uma finalidade específica que esteja fundamentada em uma das bases legais da LGPD, quais sejam:

USO E ACESSO

- fornecimento do consentimento do Titular permitindo o Tratamento de Dados Pessoais para a finalidade definida;
- cumprimento de obrigação legal ou regulatória;
- pela administração pública, para o Tratamento e uso compartilhado de Dados Pessoais necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual é parte o próprio Titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- atendimento aos legítimos interesses do Controlador ou de terceiro, desde que não se sobreponham aos direitos e liberdades fundamentais dos Titulares;
- proteção do crédito.

Importante

As finalidades dos Dados Pessoais coletados sempre devem ser informadas aos Titulares.

Os Dados Pessoais têm que ficar restritos a um conjunto de atividades específicas?

Sim. Os Dados Pessoais devem ficar restritos às finalidades informadas ao Titular no momento de sua coleta. **Não é possível desvirtuar as finalidades para as quais os Dados Pessoais foram coletados.**

Existe alguma diferença entre os dados de pessoas físicas e de organizações?

Sim. A LGPD tem como objeto de proteção os dados de pessoas físicas apenas, os chamados Dados Pessoais. Não se aplicam as regras da LGPD para o tratamento de dados de pessoas jurídicas. Note que **os dados pessoais dos representantes legais, empregados e outras pessoas físicas que trabalhem ou de qualquer forma façam parte da Organização são dados pessoais e estão sujeitos à LGPD**.

USO E ACESSO

Existe alguma diferença de tratamento/ cuidado a depender da área de trabalho realizada pela organização (saúde, educação, assistência social, jurídico)?

Sim. Em algumas circunstâncias, é possível que ocorra (com maior ou menor frequência) o Tratamento de **Dados Pessoais Sensíveis** (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), como por exemplo em iniciativas de inclusão racial ou de PCD.

Atenção

A depender da área, também é possível que ocorra o Tratamento de dados de crianças e adolescentes, o qual somente pode ser realizado mediante consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Para tratar estes Dados Sensíveis, é necessário justificar a finalidade com as bases legais específicas do tipo, que incluem:

- fornecimento do consentimento expresso e inequívoco do Titular;
- cumprimento de obrigação legal ou regulatória;
- pela administração pública, para o Tratamento e uso compartilhado de Dados Pessoais necessários à execução de políticas públicas previstas em leis e regulamentos;
- realização de estudos por órgão de pesquisa, garantida, sempre que possível, a Anonimização dos Dados Pessoais;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do Titular ou de terceiro;
- tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- garantia da prevenção à fraude e à segurança do Titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

ARMAZENAMENTO

Quais Dados Pessoais dos Titulares posso armazenar?

O mero armazenamento de Dados Pessoais (mesmo que não utilizados) é considerado uma atividade de Tratamento, protegida pela LGPD. Portanto, a organização sem fins lucrativos pode armazenar qualquer Dado Pessoal, desde que ela possua uma finalidade específica para esse Tratamento fundamentada em uma das bases legais previstas na LGPD.

Os Dados Pessoais coletados e armazenados também não devem exceder a finalidade para as quais foram coletados.

Dica

Se a Organização, para determinada finalidade, necessita apenas utilizar o nome e e-mail de um Titular, não há necessidade de armazenamento de Dados Pessoais adicionais como telefone e endereço. Lembramos que o **armazenamento de Dados Pessoais desnecessários aumenta os riscos da Organização em caso de eventual incidente de segurança.**

ARMAZENAMENTO

Como exceção à regra que quaisquer Dados Pessoais em relação aos quais a Organização tenha uma finalidade podem ser armazenados, lembramos que, em princípio, não é possível armazenar Dados Pessoais de crianças ou adolescentes obtidos sem o consentimento de seus pais ou responsáveis.

Importante

De forma geral, os **Dados Pessoais não devem ser armazenados por prazo indeterminado**. O prazo de armazenamento destes Dados Pessoais deve ser igualmente compatível com sua finalidade. Ou seja, uma vez atingido o objetivo pelo qual os Dados Pessoais foram coletados e utilizados, estes devem ser descartados de forma segura, salvo se existir algum motivo para sua manutenção (por exemplo, cumprimento de uma obrigação legal ou exercício regular de direitos).

Onde devo armazenar os Dados Pessoais do meu público?

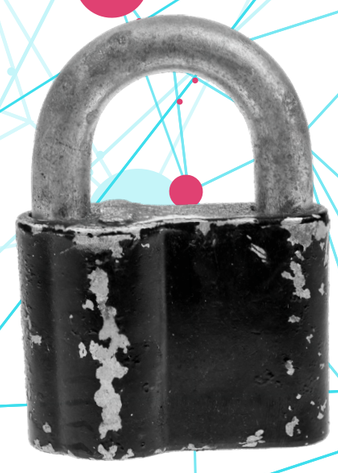
Os Dados Pessoais devem ser armazenados (seja em meio físico ou digital) em local com segurança adequada, considerando tanto ameaças internas (acessos indevidos, arquivos desprotegidos) e externas (vulnerabilidade de sistemas, invasões

hacker, vírus). Também é necessário organizar e classificar os Dados Pessoais para que, quando necessário, (a Organização possa localizá-los facilmente e consolidar as informações a serem fornecidas ao Titular (por exemplo, solicitação de cópia dos Dados Pessoais pelo Titular, pedido de retificação de Dados Pessoais, confirmação da existência de Tratamento pela Organização). A implementação de medidas de segurança é essencial para um adequado armazenamento, podendo a Organização fazer uso de diversas medidas de segurança, incluindo criptografia e Anonimização dos Dados Pessoais, quando cabível.

Dica

É importante também que os **colaboradores da Organização sejam adequada e periodicamente treinados para protegerem os Dados Pessoais e responderem de forma rápida e efetiva a qualquer incidente de segurança que envolva Dados Pessoais**. O treinamento deve incluir instruções sobre a Política de Privacidade da Organização. Recomendamos também a assinatura de acordos de confidencialidade pelos colaboradores que estabeleçam que medidas disciplinares podem ser tomadas em caso de Tratamentos de Dados Pessoais em desacordo com a LGPD ou com as políticas de Organização.

MEDIDAS DE SEGURANÇA



Quais medidas de segurança devo tomar em relação a esses Dados Pessoais?

A LGPD não lista quais medidas de segurança devem ser adotadas pelos Agentes de Tratamento. A lei menciona apenas que eles devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de Tratamento Inadequado.

Tais medidas podem incluir, mas não se limitam a:

- adoção de um programa de governança e privacidade;
- criação de uma equipe responsável pela Proteção de Dados Pessoais dentro da Organização e nomeação de um Encarregado de Proteção de Dados;
- adição dos princípios de *Privacy by Design* e *Privacy by Default* durante a execução das atividades de Tratamento de Dados Pessoais;
- criação de políticas de confidencialidade com colaboradores;

MEDIDAS DE SEGURANÇA

- estabelecimento de medidas como criptografia; firewall; senhas fortes; bloqueio de transferência e impressão de documentos. A ANPD poderá dispor sobre padrões técnicos mínimos necessários.

Dica

Uma prática essencial para evitar incidentes de segurança é a própria **classificação da relevância dos Dados Pessoais para a Organização**, permitindo o descarte de dados desnecessários e, assim, minimizando o alcance da violação.

COMPARTILHAMENTO

Como compartilhar Dados Pessoais com prestadores de serviços?

O compartilhamento de Dados Pessoais com prestadores de serviços deve ocorrer com base em uma finalidade adequada e legítima e desde que o Titular tenha ciência do compartilhamento pretendido (não é necessário especificar o nome do prestador de serviço, mas é importante que o

COMPARTILHAMENTO

Titular saiba que seus Dados Pessoais poderão ser compartilhados com terceiros e o motivo desse compartilhamento).

Dica

É importante que seja considerada a base legal mais adequada e que, a partir dessa definição, seja atendido o requisito indicado para a conformidade com a base legal. Por exemplo, caso o Tratamento seja baseado no consentimento, deverá ser criado um formulário para obtenção do consentimento específico e destacado do Titular que também deverá consentir com o compartilhamento com um terceiro.

Como Controladora dos Dados Pessoais dos Titulares, **a Organização pode ser considerada solidariamente responsável com o prestador de serviços (o Operador dos Dados Pessoais), em caso de um Tratamento inadequado por esse terceiro**, por isso é importante que a Organização:

- contrate apenas prestadores de serviço de boa reputação e com sólida capacidade financeira;
- investigue se o prestador de serviço tem um grau adequado de maturidade em relação a questões de privacidade;
- estabeleça cláusulas contratuais que especifiquem as responsabilidades, direitos e deveres das partes.

POLÍTICAS

Devo ter uma política de dados disponível para consulta em meu site?

Caso o site ou os seus serviços coletem Dados Pessoais, recomendamos a inclusão de uma Política de Privacidade em seu site. O Titular dos Dados Pessoais tem direito de saber como são utilizadas as informações coletadas e quais as finalidades da coleta. A Política de Privacidade deve, portanto, informar de forma objetiva tais aspectos, explicando ao Titular os seus direitos (acessar, retificar, solicitar a exclusão dos dados, transferir, limitar ou se opor ao Tratamento). Para garantir que o Titular foi devidamente informado, a Política de Privacidade pode conter um campo de aceite, registrando a concordância do Titular com os termos dispostos.

Quais cuidados devo ter no envio de boletins para e-mails cadastrados?

No envio de boletins para e-mails cadastrados, é necessário verificar se os Dados Pessoais que compõem a base de dados da Organização foram coletados de acordo com as exigências da LGPD, e se a atividade de envio de boletins é amparada por uma das bases legais lá previstas. Outro aspecto importante é permitir que o receptor exclua seu endereço de e-mail da lista de envio da Organização (opt-out), respeitando os direitos dos Titulares definidos na Lei. Utilizar um sistema de disparo em massa confiável também é um ponto relevante, visto que possíveis violações da ferramenta permitindo acesso à base de dados resultariam em consequências negativas para a Organização.

GLOSSÁRIO

Agentes de Tratamento: O Controlador e o Operador, conforme abaixo definido.

Anonimização: Utilização de meios técnicos razoáveis e disponíveis no momento do Tratamento por meio dos quais um Dado Pessoal perde a possibilidade de associação, direta ou indireta, a um Titular.

ANPD: Autoridade Nacional de Proteção de Dados.

Consentimento: Manifestação livre, informada e inequívoca pela qual o Titular concorda com a atividade de Tratamento de seus Dados Pessoais para uma finalidade determinada. O consentimento pode ser revogado a qualquer momento, mas não invalida Tratamentos anteriores.

Controlador: Pessoa física ou jurídica responsável pelo direcionamento e decisões relativas ao Tratamento de Dados Pessoais. Como exemplo, qualquer Organização é considerada a Controladora dos Dados Pessoais dos seus empregados.

Dados Pessoais: Informações relacionadas a uma pessoa natural identificada (e.g. nome, documento de identidade) ou identificável (e.g. perfil de consumo, score de crédito). As informações de pessoas jurídicas (e.g. CNPJ, endereço da sede corporativa) não estão protegidas pela LGPD, porém as informações dos representantes legais e demais pessoas físicas que são parte da pessoa jurídica (por exemplo nome, telefone e e-mail corporativo) estão sujeitas à LGPD.

Dados Pessoais Sensíveis: Informações 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. São informações que, se Tratadas de forma inadequada, podem gerar uma situação de discriminação ao Titular.

LGPD: Lei nº 13.0709, de 14 de agosto de 2018, também designada de Lei Geral de Proteção de Dados Pessoais. Entrou em vigor em 18 de setembro de 2020, porém as sanções administrativas lá estabelecidas somente serão eficazes a partir de agosto de 2021.

Operador: Pessoa física ou jurídica que realiza o Tratamento de Dados em nome e seguindo as instruções do Controlador. Como exemplo, um fornecedor de serviços de gerenciamento de folha de pagamento é o Operador dos Dados Pessoais dos Titulares da Organização que terceirizou essa atividade.

Titular: Pessoa Física objeto do Tratamento. Importante ressaltar que o Titular não é apenas o cliente, ou consumidor. O colaborador interno da organização, os representantes de clientes e fornecedores, também são Titulares de seus respectivos Dados Pessoais.

Tratamento: Qualquer operação realizada com Dados Pessoais, incluindo o mero acesso, coleta, armazenamento, transmissão, produção, distribuição, compartilhamento, transferência, modificação, eliminação, dentre outras atividades.

ORGANIZAÇÃO

Instituto Pro Bono

O Instituto Pro Bono é uma organização da sociedade civil que tem como missão promover o acesso à justiça por meio do fomento à advocacia voluntária e ao intercâmbio de conhecimentos jurídicos. Com o projeto Atendimento a organizações, fornece atendimento jurídico gratuito a entidades da sociedade civil por advogados e escritórios de advocacia voluntários.

Koury Lopes Advogados

O KLA é um escritório de advocacia full-service que tem como principal direcionamento estratégico o entendimento amplo e aprofundado dos negócios e dos mercados dos seus clientes para responder às suas necessidades jurídicas com precisão, agilidade, clareza nas comunicações e praticidade. Atento aos seus compromissos de responsabilidade social, o KLA tem trabalhado em parceria com diversas clearing houses em projetos pro-bono, viabilizando, dentro de sua área de influência um acesso mais democrático à Justiça.

Casa Hacker

A Casa Hacker é uma organização da sociedade civil e uma rede de espaços hackers dedicada a colocar comunidades locais no controle de suas experiências digitais e a moldarem o futuro da tecnologia da informação e comunicação para o bem público. Por meio de 8 programas desenvolvemos atividades de educação, cultura e direitos digitais para pessoas e organizações da sociedade civil periféricas.

Casa Hacker

INSTITUTO PRO BONO

KLA