

Dicas Jurídicas para
as Organizações da
Sociedade Civil:
LGPD - Lei Federal
13.709/2018

orientação 6
jurídica.

**Dicas Jurídicas para
as Organizações
da Sociedade Civil:
LGPD - Lei Federal
13.709/2018**

Projeto Orientação Jurídica

Cadernos Abong
vol. 6

Helena Duarte
Henrique B. Frota
Mauri Cruz

2021




Abong

InstitutoPólis

Brot
für die Welt

 FORD
FOUNDATION

US IDEIAS
Usinas, Ideias e Projetos

© **Abong**, 2021

Imagens

Coordenação editorial:
Danilo Feno

Projeto gráfico e editoração:
Caique Meirelles

Revisão:
Bianca Regina Fraga

Supervisão editorial
Alessandra S. O. de Proença

Apresentação
P. 09
P. 15
P. 21
P. 27
Quarta capa

| nappystock by nappy.co
| nappystock by nappy.co
| nappystock by nappy.co
| nappystock by nappy.co
| nappystock by nappy.co
| nappystock by nappy.co

Dados Internacionais de Catalogação na Publicação (CIP) (Câmara Brasileira do Livro, SP, Brasil)

Frota, Henrique B.

Dicas jurídicas para as organizações da sociedade civil [livro eletrônico] : lei geral de proteção de dados lei federal 13.709/2018 : orientação jurídica 6 / Henrique B. Frota, Helena Duarte, Mauri José Vieira Cruz. -- 6. ed. -- Porto Alegre, RS : Mauri Cruz, 2021.

(Cardenos Abong, 6).

Bibliografia.

ISBN 978-65-00-37136-9

1. Direito à privacidade 2. Proteção de dados - Direito - Brasil 3. Proteção de dados - Leis e legislação 4. Proteção de dados pessoais I. Duarte, Helena. II. Cruz, Mauri José Vieira. III. Título IV. Série.

CDU-342.721(09456)

21-96373

É vedada a reprodução de qualquer parte deste livro sem a expressa autorização da editora.

Todos os direitos reservados à ABONG



@associação.abong
@abong_osc
www.abong.org.br

ABONG

Organizações em Defesa
dos Direitos e Bens Comuns

Rua General Jardim, 660 - Cj. 81
São Paulo - SP - 01223-010
abong@abong.org.br
+55 11 3237-2122



Apresentação



**Lei Geral de Proteção de Dados
- Colocando a questão**



**Perguntas e respostas sobre a Lei Geral de
Proteção de Dados**

- | | | |
|-----|--|----|
| 1. | A Lei Geral de Proteção de Dados já está em vigor? | 14 |
| 2. | As Organizações da Sociedade Civil estão sujeitas à Lei Geral de Proteção de Dados? | 14 |
| 3. | Quais os casos em que não se aplica o tratamento de dados previstos na Lei 13.709/2018? | 15 |
| 4. | A Lei Geral de Proteção de Dados protege dados mantidos em meios físicos e digitais? | 15 |
| 5. | Quais dados são protegidos pela Lei Geral de Proteção de Dados? | 16 |
| 6. | Quais as categorias de dados que existem? | 16 |
| 7. | Quem é o/a titular dos dados? | 16 |
| 8. | Quais os princípios do tratamento de dados pessoais? | 17 |
| 9. | O que são dados pessoais? | 19 |
| 10. | O que são dados pessoais sensíveis? | 19 |
| 11. | O que é o tratamento de dados? E o que é o banco de dados? | 19 |
| 12. | Em quais hipóteses é permitido realizar o tratamento de dados pessoais? | 20 |
| 13. | Em quais hipóteses é permitido realizar o tratamento de dados sensíveis? | 22 |
| 14. | O que as Organizações da Sociedade Civil devem saber sobre o consentimento do tratamento de dados? | 23 |

15.	As Organizações da Sociedade Civil precisam pedir consentimento de todos/as os/as titulares sempre que for tratar de dados?	23
16.	Como se dá o tratamento de dados de crianças e adolescentes?	24
17.	O que é o processo de anonimização? E o que são dados anonimizados?	24
18.	Qual a diferença entre o bloqueio e a eliminação dos dados?	25
19.	O que é o uso compartilhado de dados e quando a transferência internacional de dados é permitida?	25
20.	Organizações podem se negar a compartilhar dados que sejam desnecessários ou sem finalidade específica?	26
21.	O que é o/a controlador/a, o/a encarregado/a e o/a operador/a?	27
22.	Como deve ser feita a indicação do/a encarregado/a pelo tratamento de dados pessoais?	28
23.	O que é um incidente de proteção de dados?	28
24.	Quem é responsável quando ocorre um incidente de proteção de dados?	29
25.	O que fazer quando ocorre um incidente de proteção de dados?	30
26.	O que é o relatório de impacto à proteção de dados pessoais?	31
27.	Quais os direitos dos/as titulares de dados?	31
28.	Como o/a titular pode requerer os seus direitos? Qual o prazo de resposta?	33
29.	Por quanto tempo a lei determina que deve durar o tratamento de dados?	33
30.	Quando termina o tratamento de dados?	34
31.	As Organizações da Sociedade Civil podem ter regras de boas práticas e de governança ou programa de governança em privacidade?	35

32.	Quais documentos são recomendados para as Organizações da Sociedade Civil se adequarem à Lei Geral de Proteção de Dados?	36
33.	Os documentos devem ser encaminhados para a Autoridade Nacional de Proteção de Dados revisar e aprovar?	37
34.	O que é a Autoridade Nacional de Proteção de Dados (ANPD)? Quando ela foi criada?	37
35.	Qual a competência da Autoridade Nacional de Proteção de Dados (ANPD)?	39
36.	Como se dá a participação popular na Autoridade Nacional de Proteção de Dados?	41
37.	As Organizações da Sociedade Civil e outras pessoas jurídicas ou físicas que realizem atividades de tratamento de dados pessoais devem transferir para a autoridade nacional seus bancos de dados?	41
38.	Como são aplicadas as sanções da Lei Geral de Proteção de Dados?	41
39.	Qual o tratamento que se deve ter com os documentos físicos?	43
40.	Como deve ser feito o tratamento de dados pessoais de trabalhadores/as das Organizações da Sociedade Civil? Qual o prazo que se deve manter o tratamento destes dados?	43
41.	As Organizações da Sociedade Civil podem solicitar antecedentes criminais de seus/suas trabalhadores/as?	44
42.	Como deve ser feito o tratamento de dados de documentos contábeis?	44
43.	É necessário ter alguma política específica para os cookies no website de acordo com a Lei Geral de Proteção de Dados?	45
→	Como Adequar as Organizações da Sociedade Civil à Lei Geral de Proteção de Dados	46

Modelos

ANEXO I - Modelo de Termo de Consentimento de Tratamento de Dados Pessoais

52

ANEXO II - Modelo de Política de Proteção e Tratamento de Dados Pessoais de Trabalhadores/As

55

ANEXO III - Modelo de Texto Informando a Coleta de Dados Pessoais

59

ANEXO IV - Modelo de Política de Privacidade

61

ANEXO V - Modelo de Política Interna de Proteção de Dados

71



Apresentação

Este material faz parte do
“Projeto Orientação Jurídica”,
oferecido pela Abong em parceria com
o Instituto Pólis.

O projeto tem
como **objetivos**:

Organizar e disponibilizar
em ambiente virtual as orientações
jurídicas já produzidas pela Abong,
pela Plataforma MROSC e por outras
redes e organizações parceiras;

Oferecer orientação jurídica
sobre temas relevantes para a
atuação autônoma das Organizações
da Sociedade Civil (OSC);

**Proporcionar espaços
de diálogos** entre profissionais
do Direito que atuam em apoio
às OSC e os movimentos sociais,
visando o compartilhamento de
informações e a elaboração de
teses jurídicas que fortaleçam
esta atuação;

Oferecer, em parceria com
o Instituto Pro Bono, **assessoria
jurídica gratuita** às OSC
que não disponham de recursos
para contratação;

Proporcionar a difusão
e compartilhamento de
conhecimento através das
redes sociais.



Em cada publicação abordaremos um tema específico, de forma acessível, alertando para os marcos jurídicos obrigatórios e buscando contribuir para o melhor debate em cada organização em relação as suas escolhas institucionais.

Desejamos colaborar para a consolidação de um **ambiente favorável à atuação das OSC no Brasil**, condição essencial para o fortalecimento da democracia e da justiça social em nosso país.

➤ **GT** jurídico da **Abong**



**Lei Geral de Proteção
de Dados** - Colocando
a questão





O desenvolvimento das tecnologias digitais, que cada vez mais envolve todos os âmbitos de nossas vidas, impôs um desafio para que também se avançasse uma legislação sobre o tema, visando garantir os direitos fundamentais de liberdade, intimidade e privacidade.

Em todo o mundo, países começaram a aprovar legislações específicas. Um marco na União Europeia foi a aprovação da General Data Protection Regulation (GDPR), em 2018, mudando o tratamento de dados, inclusive para empresas estrangeiras que realizam negócios com os países europeus.

No Brasil, o crescimento da produção de dados e também os episódios de vazamentos geraram uma demanda da sociedade em aprimorar a legislação vigente. Em 2014, foi aprovado o **Marco Civil da Internet (Lei 12.965/2014)**, que significou um avanço neste sentido, além da já vigente **Lei de Acesso à Informação (Lei 12.527/2010)**, que regulamenta o princípio da transparência das atividades do poder público.

Se, por um lado, a Lei de Acesso à Informação foi relevante na garantia do direito à informação e transparência da sociedade civil sobre os dados, atividades, políticas etc., dos órgãos públicos federais, estaduais e municipais, por outro lado, no ordenamento jurídico brasileiro, ainda faltava uma legislação voltada para a proteção de dados pessoais. Assim, em 2018, foi aprovada a **Lei Geral de Proteção de Dados (Lei 13.709/2018)**.

A **LGPD**, como é chamada, buscou garantir um conjunto de direitos básicos relacionados aos dados pessoais, diante da crescente digitalização das mais diversas relações de consumo. A lei apresenta regras sobre o tratamento de dados pessoais, por meios digitais ou físicos, que as empresas, organizações da sociedade civil e poder público devem seguir.

Desta forma, as atividades de coleta, armazenamento e compartilhamento de informações pessoais devem se adequar à nova lei. Para o setor das Organizações da Sociedade

Civil, a proteção de dados deve assumir uma centralidade para além dos aspectos procedimentais. Isso porque, estando a atuação da maioria das organizações na defesa, luta, garantia e implementação de direitos, é necessário compreender que a Lei Geral de Proteção de Dados é um avanço na proteção dos direitos fundamentais. Por isso, o comprometimento das organizações da sociedade civil com a proteção de dados não pode ser algo apenas mecânico mas sim ser incorporado ao cotidiano como um compromisso com a privacidade das pessoas que se relacionam de alguma forma com a organização.

É de suma importância o compromisso com uma cultura de proteção de dados, que tem como fundamentos:

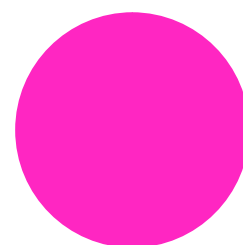
- **o respeito à privacidade;**
- **a autodeterminação informativa;**
- **a liberdade de expressão**, de informação, de comunicação e de opinião;
- **a inviolabilidade da intimidade**, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação;
- **a livre iniciativa**, a livre concorrência e a defesa do/a consumidor/a;
- **os direitos humanos**, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (**conforme Artigo 2 da Lei 13.709/2018**).

Além disso, o avanço de legislação de proteção de dados em nível mundial pode significar uma cobrança maior das empresas internacionais que se relacionam com organizações da sociedade civil brasileiras na adoção de política de proteção de dados para financiamento de projetos ou doações, por exemplo. A adequação à Lei Geral de Proteção de Dados é também uma política de transparência e boa governança, o que contribui para a imagem das organizações e no potencial de captação de recursos.



A **Lei Geral de Proteção de Dados** também contribui com a luta contra a discriminação, uma vez que garante que os dados sensíveis sejam manejados com uma maior proteção. Ao darem atenção ao tratamento de dados de forma adequada, as organizações, principalmente aquelas que trabalham com um público que sofre discriminação, colaboram na garantia de que tanto a OSC quanto as pessoas que se relacionam com ela não sejam discriminadas ou sofram perseguição político-ideológica por seu posicionamento político, orientação sexual, raça, deficiência ou qualquer outro dado sensível.

Por ser uma lei nova, a Lei Geral de Proteção de Dados ainda gera muitos questionamentos nas organizações da sociedade civil. Neste material, apresentamos as dúvidas mais frequentes sobre o tema e reunimos dicas de como adequar as políticas das OSCs a um tratamento e proteção de dados pessoais de acordo com a legislação.



Perguntas e respostas
sobre a Lei Geral de
Proteção de Dados





A Lei Geral de Proteção de Dados já está em vigor?

Sim. A **Lei 13.709/2018** foi aprovada em 14 de agosto de 2018, no entanto, ela não passou a vigorar a partir daquela data.

A própria legislação determinou um prazo para passar a vigorar em partes. Isso porque seria necessário um período de adequação de todas as pessoas físicas e jurídicas de direito privado ou público às novas regras de tratamento de dados.

A **Lei Geral de Proteção de Dados** passou então a vigorar por completo a partir de 1º de agosto de 2021, apesar da maior parte da lei já estar em vigor desde 18 de setembro de 2020. Seguem abaixo as etapas em que a lei entrou em vigor:

- **28 de dezembro de 2018:** passaram a vigorar os **artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B** (artigos que tratam da constituição da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de dados Pessoais e da Privacidade);
- **18 de setembro de 2020:** passaram a vigorar os demais artigos da Lei Geral de Proteção de Dados, com exceção dos dispositivos que tratam das sanções administrativas;
- **1º de agosto de 2021:** passaram a vigorar os **artigos 52, 53 e 54** (sanções administrativas).

As Organizações da Sociedade Civil estão sujeitas à Lei Geral de Proteção de Dados?

Sim. Os **artigos 1º e 3º da Lei 13.709/2018** estabelecem que a lei abrange o tratamento de dados pessoais realizados por pessoa natural ou por pessoa jurídica de direito privado ou público. As Organizações da Sociedade Civil são pessoas jurídicas de direito privado, em sua maioria associações privadas, e, portanto, estão sujeitas à Lei Geral de Proteção de Dados.

O **artigo 3º da Lei** define ainda que sua aplicação deve se dar para qualquer **“operação de tratamento de dado realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que”**:

- a operação de tratamento seja realizada no território nacional (**art. 3º, I da Lei 13.709/2018**);
- a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional (**art. 3º, II da Lei 13.709/2018**);
- os dados pessoais objeto de tratamento tenham sido coletados no território nacional (**art. 3º, III da Lei 13.709/2018**).



Quais os casos em que não se aplica o tratamento de dados previstos na Lei 13.709/2018?

O **artigo 4º da Lei Geral de Proteção de Dados** estabelece algumas situações nas quais não se aplica o tratamento de dados previsto na legislação, sendo elas:

- Tratamento de dados de pessoa física para fins exclusivamente particulares e não econômicos (**art. 4º, I da Lei 13.709/2018**);
- Tratamento de dados para fins exclusivamente jornalísticos ou artísticos (**art. 4º, II, a da Lei 13.709/2018**);
- Tratamento de dados para fins exclusivamente acadêmicos. Neste caso, deve-se seguir os **artigos 7º e 11º da Lei Geral de Proteção de Dados** que tratam sobre consentimento do/a titular (**art. 4º, II, b da Lei 13.709/2018**);
- Tratamento de dados para fins exclusivamente de segurança nacional, defesa nacional, segurança do Estado ou atividades de investigações e repressão de infrações penais (**art. 4º, III, a,b,c,d da Lei 13.709/2018**);
- Dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de dados pessoais adequado ao previsto na Lei Geral de Proteção de Dados (**art. 4º, IV, a da Lei 13.709/2018**).

A Lei Geral de Proteção de Dados protege dados mantidos em meios físicos e digitais?

Sim. Apesar da legislação ser motivada pela evolução do mundo digital, ela diz respeito aos dados mantidos tanto em meios digitais como físicos. Este entendimento aparece no **artigo 1º da Lei 13709/2018**: “**esta lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais**”, ou seja, abrange tanto os meios digitais como outros meios de tratamento de dados. Destaca-se que, quando a lei cita o tratamento de dados, ela não faz a distinção de qual meio.

É necessário também que as Organizações da Sociedade Civil se atentem ao tratamento de documentos físicos, como veremos mais adiante.



Quais dados são protegidos pela Lei Geral de Proteção de Dados?

A Lei garante a proteção de todos os dados cujos/as titulares são pessoas físicas, como dito, estejam eles em formato físico ou digital. Atenção: a legislação não abrange os dados titularizados por pessoas jurídicas, não considerados dados pessoais para efeito da Lei Geral de Proteção de Dados.

Quais as categorias de dados que existem?

A **Lei 13.709/2018** prevê três tipos de dados: **dados pessoais, dados pessoais sensíveis e dados pessoais de crianças e adolescentes, havendo um tratamento diferenciado para cada um, como veremos a seguir.**

Quem é o/a titular dos dados?

O/A titular é a pessoa física a qual se referem os dados pessoais que são objeto de tratamento, é a pessoa que fornece os seus dados, como CPF, RG, endereço etc. (**art. 5º, V, a da Lei 13.709/2018**).





*Quais os princípios
do tratamento de
dados pessoais?*

O primeiro princípio que baseia toda a Lei Geral de Proteção de Dados é o da boa-fé, que significa uma conduta correta e adequada para agir em sociedade e relaciona-se com os valores éticos e a transparência. A partir da boa-fé é importante ter deveres como coerência, informação e cooperação. Na Lei Geral de Proteção de Dados, a boa-fé está vinculada com o compromisso ao tratamento de dados adequado e ao cumprimento dos outros princípios estabelecidos na legislação.

Assim, o **artigo 6º da Lei Geral de Proteção de Dados** estabelece que, além do princípio da boa-fé, as atividades de tratamento de dados devem seguir os seguintes princípios:

- **Finalidade:** é o motivo do tratamento de dados que a organização realiza, ou seja, é necessário uma justificativa razoável para a coleta e utilização dos dados pessoais, caso contrário, o tratamento é considerado inadequado. A finalidade deve ser informada ao/à titular no momento de captação das informações e em momento posterior caso haja alguma alteração. De acordo com a Lei Geral de Proteção de Dados, o princípio da finalidade é definido como o tratamento de dados que deve ser feito para fins legítimos, específicos, explícitos e informados ao/à titular, sendo que não se pode dar um tratamento posterior aos dados de forma incompatível com essas finalidades (**art. 6º, I da Lei 13.709/2018**);
- **Adequação:** é a busca por meios mais adequados para realizar a coleta e o tratamento de dados pessoais de acordo com a situação específica. De acordo com a Lei, o tratamento deve ser compatível com as finalidades que foram informadas ao/à titular, de acordo com o contexto do tratamento (**art. 6º, II da Lei 13.709/2018**);
- **Necessidade:** o tratamento de dados deve se limitar ao mínimo necessário para a realização de suas finalidades. A abrangência dos dados deve ser pertinente, proporcional e não excessiva em relação ao cumprimento de suas finalidades (**art. 6º, III da Lei 13.709/2018**). Este princípio está relacionado à finalidade, assim, as organizações devem refletir quais dados são indispensáveis para o cumprimento da finalidade e coletar apenas a partir desta necessidade;
- **Livre acesso:** garantia para os/as titulares consultarem de maneira fácil e gratuita a forma e duração do tratamento, além de consulta aos seus dados de maneira integral (**art. 6º, IV da Lei 13.709/2018**). Para garantir o acesso, as organizações devem criar um fluxo e responsáveis por esta demanda, além de divulgar como se dá este acesso;



- **Qualidade dos dados:** garantia aos/às titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com as necessidades e finalidades do tratamento (art. 6º, V da Lei 13.709/2018). As Organizações da Sociedade Civil têm responsabilidade de garantir que as informações de seu banco de dados estão atualizadas, corretas e coerentes com a realidade. Para isso, é importante estabelecer mecanismos que permitam uma atualização dos dados pessoais;
- **Transparência:** garantia para os/as titulares de informações de forma clara, precisa e de fácil acesso sobre a realização do tratamento e dos respectivos agentes de tratamento, observando os segredos comercial e industrial (art. 6º, VI da Lei 13.709/2018). É uma obrigação das organizações serem transparentes sobre o modo de tratamento de dados que adota, tanto para os/as titulares como para os parceiros e para a Autoridade Nacional de Proteção de Dados (ANPD);
- **Segurança:** deve-se utilizar medidas técnicas e administrativas que sejam aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6º, VII da Lei 13.709/2018). Os dados devem ser protegidos e acessados apenas pelas pessoas e finalidades informadas aos/às titulares. Este princípio se relaciona com todo o texto da legislação, já que um dos principais objetivos é a prevenção de vazamentos e danos causados por tratamento de dados inadequados;
- **Prevenção:** deve-se adotar medidas para prevenir a ocorrência de danos decorrentes do tratamento de dados pessoais (art. 6º, VIII da Lei 13.709/2018), este princípio está relacionado ao anterior;
- **Não discriminação:** o tratamento de dados não pode ser realizado para fins discriminatórios ilícitos ou abusivos (art. 6º, IX da Lei 13.709/2018), ou seja, nenhum dado pode ser utilizado para tratamento desigual, sendo que se deve ter ainda mais atenção com os dados sensíveis, como veremos abaixo;
- **Responsabilização e prestação de contas:** é a responsabilidade de documentar os fluxos do tratamento de dados, como de demonstrar como é feita a coleta de dados, qual a finalidade, como são feitos o compartilhamento e armazenamento etc. Essas informações podem ser informadas aos/às titulares, parceiros e Autoridade Nacional de Proteção de Dados (ANPD), que têm direito de saber sobre os procedimentos. A Lei define este princípio como o dever de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (art. 6º, X da Lei 13.709/2018).



O que são dados pessoais?

O **Artigo 5º, I da Lei Geral de Proteção de Dados** conceitua dados pessoais como: “**informação relacionada à pessoa natural identificada ou indetectável**”, que são todos aqueles dados que podem identificar uma pessoa, a exemplo: **RG, CPF, título de eleitor, telefone, endereço, link de perfil nas redes sociais etc.** Esses dados podem ser uma informação isolada, que pode identificar o/a titular, ou, ainda, um conjunto de dados que geram informações combinadas e permitem que uma pessoa seja identificada.

O que são dados pessoais sensíveis?

Os dados sensíveis são todos aqueles que se relacionam com a vida pessoal do/a titular e que podem gerar situações delicadas, discriminação ou constrangimentos. Por isso, são dados que necessitam de uma proteção maior em seu tratamento. O **Artigo 5º, II da Lei 13.709/2018** define dados sensíveis como: “**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**”.

É importante frisar que o rol do **Artigo 5º, II da Lei 13.709/2018** é exemplificativo, ou seja, os dados sensíveis são apurados e classificados a partir do caso concreto. A legislação não cita, por exemplo, dados sobre orientação sexual ou identidade de gênero, porém esses dados devem ser considerados sensíveis já que podem ser utilizados de forma discriminatória.

O que é o tratamento de dados?

E o que é o banco de dados?

De forma simples, o tratamento de dados é tudo aquilo que se faz com a informação, desde o momento da coleta até o momento da sua exclusão. O **Artigo 5º, X da Lei 13.709/2018** determina que tratamento de dados é “**toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração**”.

Lembrando que este rol é taxativo.

Já o banco de dados é o “conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, suporte eletrônico ou físico” (**Artigo 5º, IV da Lei 13.709/2018**).



Destaca-se que o uso compartilhado de dados entre duas instituições também é considerado tratamento de dados, sendo este a comunicação, difusão, transferência internacional ou tratamento compartilhado de bancos de dados pessoais. Nessas situações, as duas pessoas jurídicas envolvidas no compartilhamento se responsabilizam pelos direitos de titulares.

Desta forma, podemos perceber que toda organização trabalha de alguma forma com tratamento de dados, não importando a área de atuação ou tamanho. Evidente que há diferenças: há organizações com um grande fluxo de dados e outras não, mas toda associação possui ao menos os dados de associados/as, diretores/as, conselheiros/as, trabalhadores/as, entre outros.

Em quais hipóteses é permitido realizar o tratamento de dados pessoais?

A Lei Geral de Proteção de Dados estabeleceu algumas hipóteses nas quais se justifica a captação e o tratamento de informações pessoais, sendo elas:

- **Consentimento:** é quanto o/a titular autoriza o uso de seus dados (Art. 7º, I da Lei 13.709/2018). O consentimento deve ser feito de forma a garantir e documentar que o/a titular entendeu a finalidade do tratamento de seus dados e o autorizou de forma livre e consciente. Nas questões seguintes, veremos mais a fundo o tema do consentimento;
- **Obrigação legal:** é o tratamento de dados a partir da permissão ou imposição de uma lei, norma, regulamento ou portaria administrativa. Para facilitar o entendimento, pode ser dado o exemplo da documentação de trabalhadores/as que são determinados na Consolidação das Leis Trabalhistas – CLT para efetivar a relação de emprego. Vale destacar que o tratamento de dados a partir de obrigação legal deve respeitar o prazo (Art. 7º, II da Lei 13.709/2018);
- **Execução de políticas públicas:** o poder público pode realizar o tratamento de dados visando a execução de políticas públicas (Art. 7º, III da Lei 13.709/2018);
- **Realização de estudos por órgão de pesquisa:** os órgãos ou instituições de pesquisa podem utilizar dados para atingir as suas finalidades. Vale destacar que as instituições ou órgãos devem ter como objeto social, no Cadastro Nacional de Pessoa Jurídica – CNPJ, a realização de pesquisas,



podendo ser o único objeto social ou estar combinado com outros. Neste, deve-se garantir sempre que possível a anonimização dos dados (Art. 7º, IV da Lei 13.709/2018);

- **Execução de um contrato assinado pelo/a titular de dados:** é a captação de dados necessários para cumprir uma obrigação de contrato entre o/a controlador/a e o/a titular de dados (Art. 7º, V da Lei 13.709/2018);
- **Exercício regular do direito em processo judicial, administrativo ou arbitral:** um/a titular de dados ou uma pessoa jurídica pode acessar informações armazenadas com o objetivo de fazer um processo judicial, administrativo ou arbitral contra terceiros/as (Art. 7º, VI da Lei 13.709/2018);
- **Para a proteção da vida ou incolumidade do/a titular ou de terceiro/a:** permite-se a utilização de dados pessoais para a proteção de pessoas que estejam em risco de vida ou de violência física. Neste caso, é possível inclusive usar dados sensíveis (Art. 7º, VII da Lei 13.709/2018);
- **Para a tutela da saúde:** exclusivamente os/as profissionais, serviços ou autoridades sanitárias podem tratar dados pessoais com objetivo de tratamentos e serviços que visam a saúde do/a titular (Art. 7º, VIII da Lei 13.709/2018);
- **Em razão de legítimo interesse do/a controlador/a:** esta justificativa é mais ampla, mas deve ser feita a partir da identificação sobre a finalidade do tratamento de dados e de qual interesse da organização neste procedimento (Art. 7º, IX da Lei 13.709/2018). O artigo 10 da Lei Geral de Proteção de Dados estabelece que as finalidades devem ser legítimas nesta situação e consideradas a partir do caso concreto. O artigo inclui exemplos não taxativos de tratamento de dados em razão do interesse do/a controlador/a, sendo: para apoio e promoção de atividades do/a controlador/a, proteção do exercício regular dos direitos do/a titular e prestação de serviços que beneficiam o/a titular. O Artigo 10 também determina, em seus parágrafos 1º, 2º e 3º, que neste caso deve-se utilizar dados estritamente necessários para a finalidade, que o/a controlador/a deve adotar medidas garantidoras da transparência e que a autoridade nacional pode solicitar relatório de impacto à proteção de dados pessoais;
- **Para a proteção do crédito:** as instituições financeiras podem fazer tratamento de dados dos/as titulares com objetivo de proteger o crédito que irão fornecer (Art. 7º, X da Lei 13.709/2018).



*Em quais hipóteses
é permitido realizar
o tratamento de
dados sensíveis?*

Os dados sensíveis, em via de regra, só podem ser tratados com o consentimento do/a titular de forma específica e destacada para finalidade específica (**Artigo 11, I da Lei 13.709/2018**). No entanto, a Lei Geral de Proteção e Dados determina algumas hipóteses em que é permitido o tratamento de dados sensíveis, desde que sejam indispensáveis para:

- **Cumprimento de obrigação legal** ou regulatória pelo/a controlador/a (**Artigo 11, II, a da Lei 13.709/2018**);
- **Para execução** pela administração pública de políticas públicas (**Artigo 11, II, b da Lei 13.709/2018**);
- **Realização de estudos por órgão de pesquisa:** os órgãos ou instituições de pesquisa podem utilizar dados para atingir as suas finalidades. Vale destacar que as instituições ou órgãos devem ter como objeto social, no Cadastro Nacional de Pessoa Jurídica – CNPJ, a realização de pesquisas, podendo ser o único objeto social ou estar combinado com outros. Neste, deve-se garantir sempre que possível a anonimização dos dados (**Artigo 11, II, c da Lei 13.709/2018**);
- **Exercício regular do direito em processo judicial, administrativo ou arbitral:** um/a titular de dados ou uma pessoa jurídica pode acessar informações armazenadas com o objetivo de fazer um processo judicial, administrativo ou arbitral contra terceiros/as (**Artigo 11, II, d da Lei 13.709/2018**);
- **Para a proteção da vida ou incolumidade do/a titular ou de terceiro/a:** permite-se a utilização de dados pessoais para a proteção de pessoas que estejam em risco de vida ou de violência física (**Artigo 11, II, e da Lei 13.709/2018**);
- **Para a tutela da saúde:** exclusivamente os/as profissionais, serviços ou autoridades sanitárias podem tratar dados pessoais com objetivo de tratamentos e serviços que visam a saúde do/a titular (**Artigo 11, II, f da Lei 13.709/2018**);
- **Para a prevenção de fraudes e para segurança** do/a titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (**Artigo 11, II, g da Lei 13.709/2018**).



O que as Organizações da Sociedade Civil devem saber sobre o consentimento do tratamento de dados?

O consentimento é a manifestação livre, informada e inequívoca pela qual o/a titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (**Artigo 5º, XII da Lei 13.709/2018**). É importante que o consentimento não seja apenas um ato formal, mas que haja garantias de que a pessoa entendeu a finalidade do uso de seus dados e que consentiu de forma livre. Para isso, é essencial a adoção de mecanismos tecnológicos e também de uma linguagem simples e acessível.

A legislação determina que o consentimento deve se dar de forma escrita e a finalidade deve estar em uma cláusula destacada (**Artigo 8º, § 1º da Lei 13.709/2018**). Caso, no texto do consentimento, a finalidade não esteja determinada e seja genérica, o consentimento é considerado nulo (**Artigo 8º, § 4º da Lei 13.709/2018**) e não é possível realizar o tratamento de dados.

É um direito do/a titular a revogação de seu consentimento a qualquer momento, esta que deve ser feita através de manifestação expressa por meio de procedimento gratuito e facilitado (**Artigo 8º, § 5º da Lei 13.709/2018**). Nesta situação, os dados devem ser eliminados.

Quando há uma mudança no tratamento de dados em relação a finalidade, forma e duração, identidade do/a controlador/a ou compartilhamento de dados, a informação sobre a alteração deve ser dada ao/à titular pelo/a controlador/a. O/A titular pode revogar seu consentimento caso não concorde com a mudança realizada (**Artigo 8º, § 6º da Lei 13.709/2018**).

As Organizações da Sociedade Civil precisam pedir consentimento de todos/as os/as titulares sempre que for tratar de dados?

Não. Como visto anteriormente, há algumas situações em que a legislação permite o tratamento de dados sem consentimento, como para execução de políticas públicas ou para cumprimento de obrigações contratuais, entre outras. No entanto, caso não haja uma justificativa prevista em lei, é necessário o consentimento do/a titular.



*Como se dá o
tratamento de
dados de crianças
e adolescentes?*

Em relação aos dados de crianças e adolescentes, o **artigo 14 da Lei Geral de Proteção de Dados** define algumas regras, principalmente ao que diz respeito ao consentimento. Nos casos de tratamento de dados de menores de idade, é necessário que o consentimento seja dado de forma específica e em destaque por pelo menos um dos pais ou responsáveis legais (**§ 1º do Artigo 14 da Lei 13.709/2018**). É responsabilidade do/a controlador/a assegurar que o consentimento, principalmente os por meios digitais, foi dado pelos pais ou responsáveis legais da criança ou adolescente (**§ 5º do Artigo 14 da Lei 13.709/2018**).

Nos casos de tratamento de dados de crianças e adolescentes, as informações sobre o tipo de dados coletados, a forma de sua utilização e os procedimentos devem ser públicas e serem fornecidas de maneira simples, clara e acessível (**§ 1º e § 6º do Artigo 14 da Lei 13.709/2018**).

A legislação prevê apenas uma hipótese em que os dados de crianças e adolescentes possam ter seus dados coletados sem o consentimento dos pais ou responsável legal, no caso quando há a necessidade de coleta justamente para contatar os pais ou responsáveis legais. Nesta situação, o dado deve ser utilizado esta única vez, sem armazenamento, não podendo ser repassados para terceiros/as.

Um ponto interessante da Lei Geral de Proteção de Dados sobre dados de menores de idade é que a legislação proíbe que os/as controladores/as condicionem a participação em jogos, aplicativos ou outras atividades ao fornecimento de informações pessoais. Nesses casos, os dados exigidos devem ser apenas aqueles necessários à atividade (**§ 4º do Artigo 14 da Lei 13.709/2018**).

*O que é o processo
de anonimização?
E o que são dados
anonimizados?*

O processo de anonimização é um procedimento que quebra a ligação entre o/a titular de dados e as informações sobre ele/a, de forma que impeça a identificação da pessoa a partir dos dados pessoais. Um exemplo é a utilização de estatísticas, entre outros. O **Artigo 5º, XI da Lei Geral de Proteção de Dados** define como: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação direta ou indireta a um indivíduo.

Desta forma, os dados anonimizados é o dado relativo a titular que não possa ser identificado/a, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (**Artigo 5º, III da Lei 13.709/2018**).



Qual a diferença entre o bloqueio e a eliminação dos dados?

O bloqueio de informações é a “**suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados**” (Artigo 5º, XIII da Lei 13.709/2018) e pode acontecer a partir da solicitação do/a titular ou ser uma sanção.

Já a eliminação é a “**exclusão de dados ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado**” (Artigo 5º, XIV da Lei 13.709/2018).

A exclusão é definitiva e pode ocorrer também por requerimento do/a titular ou ser uma sanção.

O que é o uso compartilhado de dados e quando a transferência internacional de dados é permitida?

O uso compartilhado de dados foi definido no Artigo 5º, XVI da Lei Geral de Proteção de Dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados. Já a transferência internacional de dados é a transmissão de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (Artigo 5º, XV da Lei 13.709/2018).

A transferência internacional de dados é permitida apenas nas situações previstas no Artigo 33 da Lei Geral de Proteção de Dados, sendo elas:

- Para países ou organismos internacionais que proporcionem grau de **proteção de dados pessoais** adequado ao previsto na Lei Geral de Proteção de Dados. Sendo que cabe a Autoridade Nacional de Proteção de Dados avaliar esta adequação (Artigo 33, I e Artigo 34 da Lei 13.709/2018);
- Quando o/a controlador/a **oferecer e comprovar** garantias de cumprimento dos princípios, dos direitos do/a titular e do regime de proteção de dados previstos na Lei, na forma de:
 - a) cláusulas contratuais específicas para determinada transferência;
 - b) cláusulas-padrão contratuais;
 - c) normas corporativas globais;
 - d) selos, certificados e códigos de conduta regularmente emitidos (Artigo 33, II da Lei 13.709/2018);



- Quando a transferência for necessária para a **cooperação jurídica internacional** entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional (**Artigo 33, III da Lei 13.709/2018**);
- Quando a transferência for necessária para a **proteção da vida ou da incolumidade física** do/a titular ou de terceiro/a (**Artigo 33, IV da Lei 13.709/2018**);
- Quando a autoridade nacional **autorizar** a transferência (**Artigo 33, V da Lei 13.709/2018**);
- Quando a transferência resultar em **compromisso assumido em acordo de cooperação internacional** (**Artigo 33, VI da Lei 13.709/2018**);
- Quando a transferência for necessária para a **execução de política pública** ou atribuição legal do serviço público (**Artigo 33, VII da Lei 13.709/2018**);
- Quando o/a titular tiver fornecido seu **consentimento específico** e em destaque para a transferência internacional, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades (**Artigo 33, VIII da Lei 13.709/2018**);
- **Quando necessário para atender as hipóteses:** obrigação legal, para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o/a titular ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral (**Artigo 33, IX da Lei 13.709/2018**).

Organizações podem se negar a compartilhar dados que sejam desnecessários ou sem finalidade específica?

Sim. Muitas vezes, as Organizações da Sociedade Civil precisam compartilhar dados com parceiros/as internacionais ou em parcerias com o poder público, como na prestação de contas de um projeto, para comprovar participação em atividades, entre outros. Nessas situações, as organizações podem se negar a compartilhar dados que sejam desnecessários ou que não tenham uma finalidade específica. Em relação à prestação de contas, o **Marco Regulatório das Organizações da Sociedade Civil (Lei 13.019/2014)** determina que esta deve estar relacionada à comprovação das metas e resultados, e não a notas e recibos fiscais (**Artigo 64 da Lei 13.019/2014**). Assim, um dos argumentos a ser utilizados é o cumprimento dos princípios da Lei Geral de Proteção de Dados.



O que é o/a controlador/a, o/a encarregado/a e o/a operador/a?

O/A controlador/a é a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (**Artigo 5º, VI da Lei 13.709/2018**). No caso das Organizações da Sociedade Civil, o/a controlador/a é o órgão diretivo responsável por definir a política de proteção de dados.

O/A encarregado/a é pessoa indicada pelo/a controlador/a e operador/a para atuar como canal de comunicação entre o/a controlador/a, os/as titulares dos dados e a **Autoridade Nacional de Proteção de Dados (ANPD)** (**Artigo 5º, VIII da Lei 13.709/2018**). A Lei Geral de Proteção de Dados determina que o/a encarregado/a indique o/a encarregado/a para o tratamento de dados pessoais (**Artigo 41 da Lei 13.709/2018**).

As atividades do/a encarregado/a são:

- **aceitar** reclamações e comunicações dos/as titulares, prestar esclarecimentos e adotar providências;
- **receber** comunicações da Autoridade Nacional de Proteção de Dados e adotar providências;
- **orientar** os/as funcionários/as e os/as contratados/as da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- **executar** as demais atribuições determinadas pelo/a controlador/a ou estabelecidas em normas complementares (**Artigo 41, § 2º da Lei 13.709/2018**). A identidade do/a encarregado/a e o seu contato deve ser divulgado publicamente, de forma clara e objetiva, de preferência no site da Organização da Sociedade Civil (**Artigo 41, § 1º da Lei 13.709/2018**).

Vale destacar que tanto o/a controlador/a como o/a encarregado/a precisam fazer registro das operações de tratamento de dados pessoais, principalmente na hipótese do tratamento ocorrer devido ao seu legítimo interesse, já citada do **Artigo 7º, IX da Lei 13.709/2018**.

Por fim, o/a operador/a é a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais a partir das instruções do/a controlador/a (**Artigo 5º, VII da Lei 13.709/2018**).



Como deve ser feita a indicação do/a encarregado/a pelo tratamento de dados pessoais?

Como já visto, o/a encarregado/a deve ser indicado/a pelo/a controlador/a e tal informação deve ser divulgada publicamente de forma clara e objetiva, de preferência no site do/a controlador/a (**Artigo 41, § 1º da Lei 13.709/2018**). Para além disso, não há nenhuma previsão legal, até o momento, para que os dados do/a encarregado/a sejam encaminhados para a **Autoridade Nacional de Proteção de Dados (ANPD)**. Assim, basta as Organizações da Sociedade Civil definirem os/a encarregados/as e divulgarem em seu sites ou outros meios eletrônicos. Vale destacar que também não há nenhuma exigência de que o/a encarregado/a tenha uma certificação profissional.

O que é um incidente de proteção de dados?

Um incidente de segurança é todo acontecimento que pode comprometer a segurança de dados pessoais. O incidente pode levar a destruição, perda, alteração, divulgação, acesso não autorizado ou venda ilegal de dados pessoais. Pode ocorrer de forma acidental ou ilícita. Já o vazamento de dados é o nome dado para um tipo de incidente de segurança que envolve especificamente a exposição não autorizada de dados pessoais e informações privadas e sigilosas para terceiros sem autorização ou de forma pública.





**Quem é responsável
quando ocorre
um incidente de
proteção de dados?**

Há um tratamento irregular ou ilícito, pela Lei Geral de Proteção de Dados, quando o/a controlador/a não segue os parâmetros legais em relação à finalidade do tratamento, técnicas adotadas, resultado ou riscos envolvidos (**artigo 44 da Lei 13.709/2018**). Vale destacar que o incidente de proteção de dados pode ocorrer mesmo que a OSC faça um tratamento de dados conforme a legislação.

Para uma responsabilização, é necessário que haja pessoas prejudicadas que tenham sofrido um dano e que haja uma ligação entre o dano e a conduta do/a controlador/a e/ou operador/a. Nessas situações, o/a controlador/a é responsabilizado/a pelos danos causados devendo repará-los de forma indenizatória (**Artigo 42, I da Lei 13.709/2018**), sendo que o/a operador/a pode responder de forma solidária quando tiver descumprido as obrigações da legislação ou as instruções do/a controlador/a (**Artigo 42, II da Lei 13.709/2018**). Nos casos em que há mais de uma organização envolvida no tratamento de dados, todas respondem pelo incidente de forma solidária.

Vale destacar que o/a controlador/a e o/a operador/a **não são responsabilizados** quando provarem que:

- Não realizaram o tratamento de dados pessoais que lhes é atribuído (**Artigo 43, I da Lei 13.709/2018**);
- Não houve violação à Lei Geral de Proteção de Dados, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído (**Artigo 43, II da Lei 13.709/2018**);
- O dano decorrente de culpa exclusiva do/a titular ou de terceiro/a (**Artigo 43, III da Lei 13.709/2018**).

Por fim, quando ocorre um incidente de proteção de dados, a autoridade nacional pode aplicar sanções previstas na legislação, como veremos abaixo.



**O que fazer quando
ocorre um incidente
de proteção de
dados?**

Como já foi dito, as organizações devem adotar medidas de segurança para proteger os dados pessoais e banco de dados, sendo este um princípio muito importante da legislação. Além disso, recomenda-se que a política interna de proteção de dados das OSCs contenha orientações de como proceder nos incidentes de proteção de dados. No documento, deve conter orientações para o/a encarregado/a e equipe atuarem caso aconteça um **incidente; definir responsáveis para atuar junto ao/à encarregado/a nessas situações; entre outras orientações que a OSC optar.**

Os incidentes podem ocorrer mesmo com todas as medidas de adequação à Lei, o mais importante é que a OSC tenha adotado medidas de prevenção e reaja de uma forma boa e rápida.

Quando ocorre uma ocorrência ou incidente de segurança que pode vir a gerar um risco ou dano aos/às titulares, a legislação determina que o/a controlador/a deve comunicar, em prazo razoável, a Autoridade Nacional de Proteção de Dados e o/a titular sobre a ocorrência. Esta comunicação deve conter, no mínimo:

- A descrição da natureza dos dados pessoais afetados (Artigo 48, § 1º, I da Lei 13.709/2018);
- As informações sobre os/as titulares envolvidos/as (Artigo 48, § 1º, II da Lei 13.709/2018);
- A indicação das medidas técnicas e da segurança utilizadas para a proteção dos dados, observador os segredos comercial e industrial (Artigo 48, § 1º, III da Lei 13.709/2018);
- Os riscos relacionados ao incidente (Artigo 48, § 1º, IV da Lei 13.709/2018);
- Os motivos da demora, no caso de a comunicação não ter sido imediata (Artigo 48, § 1º, V da Lei 13.709/2018);
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (Artigo 48, § 1º, VI da Lei 13.709/2018).

A **Autoridade Nacional de Proteção de Danos** tem o dever de verificar a gravidade do incidente e, quando for o caso, determinar a adoção de alguma outra providência. A Lei apresenta dois exemplos para isso: ampla divulgação do fato em meios de comunicação ou medidas para reverter os efeitos do incidente (Artigo 48, § 2º, I e II da Lei 13.709/2018). Para aplicar as sanções, a autoridade nacional considera o fato das organizações terem adotado mecanismos para evitar o incidente, as boas práticas de governança e também a agilidade de resposta ao ocorrido.



O que é o relatório de impacto à proteção de dados pessoais?

Já foi dito que tanto o/a controlador/a como o/a encarregado/a devem manter registro dos procedimentos realizados durante o tratamento de dados pessoais. O relatório de impacto à proteção de dados pessoais é a documentação do/a controlador/a que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (**Artigo 5º, XVII da Lei 13.709/2018**).

A Autoridade Nacional de Proteção de Dados (ANPD) pode determinar a elaboração deste relatório pelo/a controlador/a, inclusive de dados sensíveis (**Artigo 38 da Lei 13.709/2018**).

De acordo com o parágrafo único do **Artigo 38 da Lei 13.709/2018**, o relatório deve conter no mínimo:

- A descrição dos tipos de dados coletados;
- A metodologia utilizada para a coleta e para a garantia da segurança das informações;
- A análise do/a controlador/a sobre as medidas, salvaguardas e mecanismos visando a mitigação dos riscos.

Quais os direitos dos/as titulares de dados?

Toda pessoa tem direito à titularidade de seus dados pessoais, além da garantia da liberdade, intimidade e privacidade (**Artigo 17 da Lei 13.709/2018**), direitos fundamentais que são basilares da Lei Geral de Proteção de Dados.

O **artigo 18 da Lei 13.709/2018** estabelece alguns direitos que os/as titulares dos dados pessoais têm de obter do/a controlador/a sobre o tratamento de seus dados, a qualquer momento e mediante requisição. Esses direitos são:

- ↗ **Confirmação da existência de tratamento:** essa confirmação pode ser respondida de imediato pela OSC com um aviso sobre a finalidade e duração do armazenamento ou respondida em até 15 dias com uma declaração completa com a origem dos dados, existência de registro, critérios utilizados para coleta e finalidade do tratamento (**Artigos 18, I e 19 da Lei 13.709/2018**);



- **Acesso aos dados:** essa confirmação pode ser respondida de imediato pela OSC com um aviso sobre a finalidade e duração do armazenamento ou respondida em até 15 dias com uma declaração completa com a origem dos dados, existência de registro, critérios utilizados para coleta e finalidade do tratamento (**Artigos 18, II e 19 da Lei 13.709/2018**);
- **Correção de dados** incompletos, inexatos ou desatualizados (**Artigo 18, III da Lei 13.709/2018**);
- **Anonimização, bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados (**Artigo 18, IV da Lei 13.709/2018**);
- **Portabilidade dos dados** a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial (**Artigo 18, V da Lei 13.709/2018**);
- **Eliminação dos dados** pessoais tratados com o consentimento do/a titular, exceto nas hipóteses em que é permitido a conservação dos dados previstos no Artigo 16 da Lei 13.709/2018 que veremos mais adiante (**Artigo 18, VI da Lei 13.709/2018**);
- **Informação das entidades** públicas e privadas com as quais o/a controlador/a realizou uso compartilhado de dados (**Artigo 18, VII da Lei 13.709/2018**);
- Informação sobre a **possibilidade de não fornecer consentimento** e sobre as consequências negativas (**Artigo 18, VIII da Lei 13.709/2018**);
- **Revogação do consentimento** a qualquer momento (**Artigo 18, IX da Lei 13.709/2018**).

Sobre o tratamento de seus dados, o/a titular tem direito ao acesso facilitado às seguintes informações: **finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do/a controlador/a; informações acerca do uso compartilhado de dados pelo/a controlador/a e a finalidade; responsabilidades dos/as agentes que realizam o tratamento; direitos do/a titular** (**Artigo 9 da Lei 13.709/2018**).



**Como o/a titular
pode requerer
os seus direitos?
Qual o prazo
de resposta?**

Para reivindicar os seus direitos previstos na lei, o/a titular deve fazer um requerimento expresso ou através de representante legalmente constituído para o/a controlador/a ou encarregado/a. A resposta em relação a tais direitos deve ser feita de maneira imediata. Quando não for possível a adoção imediata de providências, o/a controlador/a deve comunicar que não é o/a agente de proteção de dados e indicar o/a verdadeiro/a agente ou explicar por que não pode tomar providências imediatamente expondo as razões de fato ou de direito (**Artigo 18, § 4º, I e II da Lei 13.709/2018**).

Em relação à confirmação do tratamento de dados ou acesso aos dados pessoais, as medidas tomadas podem ser:

- Em formato simplificado, imediatamente (**Artigo 19, I da Lei 13.709/2018**);
- Por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de 15 dias, contando da data do requerimento do/a titular (**Artigo 19, II da Lei 13.709/2018**).

**Por quanto tempo
a lei determina
que deve durar
o tratamento de
dados?**

A Lei Geral de Proteção de Dados não especifica um prazo de duração para o tratamento de dados pessoais, isso vai depender das circunstâncias específicas e da finalidade do tratamento. Em via de regra, o tratamento acaba quando a finalidade também termina, devendo os dados serem eliminados. Como veremos abaixo, a lei estabelece em quais situações há o término do tratamento de dados e quais hipóteses é permitida a conservação.



**Quando termina
o tratamento de
dados?**

O tratamento de dados pessoais encerra nas seguintes situações previstas no **artigo 15** da **Lei Geral de Proteção de Dados**:

- Quando a finalidade foi alcançada e não há mais necessidade ou pertinência de tratamento (**Artigo 15, I da Lei 13709/2018**);
- No fim do período de tratamento (**Artigo 15, II da Lei 13709/2018**);
- Com a comunicação do/a titular de que deseja revogar o seu consentimento de tratamento de seus dados (**Artigo 15, III da Lei 13709/2018**);
- A partir de determinação da autoridade nacional, quando houver violação da legislação (**Artigo 15, IV da Lei 13709/2018**).

Vale destacar que o **artigo 16** da Lei autoriza a conservação de dados pessoais após o término do tratamento para as seguintes finalidades:

- Cumprimento de obrigação legal ou regulatória pelo/a controlador/a (**Artigo 16, I da Lei 13709/2018**);
- Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (**Artigo 16, II da Lei 13709/2018**);
- Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei Geral de Proteção de Dados (**Artigo 16, III da Lei 13709/2018**);
- Para uso exclusivo do/a controlador/a, sendo vedado acesso por terceiro e desde que os dados estejam anonimizados (**Artigo 16, IV da Lei 13709/2018**).



As Organizações da Sociedade Civil podem ter regras de boas práticas e de governança ou programa de governança em privacidade?

Sim. Os/As controladores/as e operadores/as podem, a partir do volume de operações de tratamento de dados, fluxo de informações e características dos dados coletados, estabelecer regras de boas práticas ou, ainda, programa de governança em privacidade. Isso é uma opção que deve ser feita a partir da necessidade real da organização. A Lei Geral de Proteção de Dados prevê a possibilidade de regras e programas e que a autoridade nacional deverá estimular a adoção de padrões técnicos que facilitem o controle e acesso pelos/as titulares (**Artigo 51 da Lei 13.709/2018**).

As regras de boas práticas e governança podem estabelecer as condições de organização, o regime de funcionamento, os procedimentos, a forma de comunicação (inclusive de reclamação), normas de segurança, padrões técnicos, obrigações das pessoas envolvidas no tratamento, ações educativas para a equipe e mecanismos internos de supervisão e prevenção de incidentes de segurança (**Artigo 50, § 1º da Lei 13.709/2018**).

Já o programa de governança em privacidade é algo mais estruturado que surge a partir de um volume grande de operações de tratamento de dados e, de acordo com a legislação, deve ter no mínimo:

- **Comprometimento** do/a controlador/a em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais (**Artigo 50, § 2º, I, a da Lei 13.709/2018**);
- **Aplicabilidade** a todo o conjunto de dados pessoais que estejam sob o controle da organização, independentemente do modo como se realizou a coleta (**Artigo 50, § 2º, I, b da Lei 13.709/2018**);
- **Adaptação à estrutura**, à escala e ao volume das operações da organização, bem como à sensibilidade dos dados tratados (**Artigo 50, § 2º, I, c da Lei 13.709/2018**);
- **Políticas salvaguardas adequadas** com base em processo de avaliação sistemática de impactos e riscos à privacidade (**Artigo 50, § 2º, I, d da Lei 13.709/2018**);
- Objetivo de **estabelecer relação de confiança** com o/a titular, por meio de atuação transparente e que assegure mecanismos de participação do/a titular (**Artigo 50, § 2º, I, e da Lei 13.709/2018**);



Integração com a estrutura geral de governança da organização e estabelecimento e aplicação de mecanismos de supervisão internos e externos (Artigo 50, § 2º, I, f da Lei 13.709/2018);



Planos de resposta e incidentes e remediação (Artigo 50, § 2º, I, g da Lei 13.709/2018);



Atualização constante com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas (Artigo 50, § 2º, I, h da Lei 13.709/2018).

Tanto as regras de boas práticas como o programa de governança em privacidade devem ser atualizados e publicados, podendo, inclusive, serem reconhecidos e divulgados pela **Autoridade Nacional de Proteção de Dados (ANPD)** (Artigo 50, § 3º da Lei 13.709/2018).

Quais documentos são recomendados para as Organizações da Sociedade Civil se adequarem à Lei Geral de Proteção de Dados?

Para se adequarem à **Lei Geral de Proteção de Dados**, as organizações precisam alterar políticas ou manuais internos que já existam sobre tratamento de dados ou então criar do zero, caso não tenham. Não há uma regra sobre quais documentos são obrigatórios, isto vai depender das operações de dados da organização, tanto em termos de quantidade como de qualidade. É recomendado que a organização tenha, no mínimo, uma Política de Privacidade divulgada em seu site com: **nome e contato do/a encarregado/a; forma de coleta de dados; finalidade; mecanismos de proteção; se há compartilhamento de dados; período de armazenamento; entre outros**. Outro documento essencial é o termo de consentimento de tratamento de dados pessoais.

Além disso, a OSC pode ter uma Política Interna de Tratamento e Proteção de Dados com orientações para os/as trabalhadores/as e dirigentes sobre o tratamento de dados adotado pela instituição e também uma Política de Tratamento de Dados Pessoais de Trabalhadores/as, entre outros documentos que avaliar pertinentes. Ao final desta cartilha, há alguns modelos de documentos que podem ser adotados pelas Organizações da Sociedade Civil.



Os documentos devem ser encaminhados para a Autoridade Nacional de Proteção de Dados revisar e aprovar?

A **Autoridade Nacional de Proteção de Dados (ANPD)** pode, dentre suas atribuições, reconhecer e divulgar regras de boas práticas. No entanto, isso não significa que os documentos orientativos, como a política de privacidade da organização ou manuais internos, elaborados por controladores/as ou operadores/as, precisem ser avaliados e aprovados pela Autoridade Nacional antes de serem adotados.

O que é a Autoridade Nacional de Proteção de Dados (ANPD)? Quando ela foi criada?

A **Autoridade Nacional de Proteção de Dados (ANPD)** é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território nacional (**Artigo 5º, XIX da Lei 13.709/2018**). Vale destacar que a autoridade nacional tem autonomia técnica e decisória (**Artigo 55-B da Lei 13.709/2018**).

A ANPD foi criada legalmente pela **Medida Provisória nº 869/2018** que foi convertida na **Lei 13.853/2018**, mas iniciou efetivamente as suas atividades em 6 de novembro de 2020 quando foi nomeado o seu diretor-presidente.

A estrutura da ANPD possui a seguinte composição (**Artigo 55-C da Lei 13.709/2018 e Artigo 3o do Anexo I do Decreto 10.474/2020**):

- Conselho Diretor;
- Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
- Corregoria;
- Ouvidoria;
- Órgão de assessoramento jurídico próprio;
- Unidades administrativas e unidades especializadas necessárias à aplicação do disposto na Lei Geral de Proteção de Dados.

De acordo com a legislação (Artigo 55-D da Lei 13.709/2018), o Conselho Diretor é o órgão máximo de direção da Autoridade Nacional de Proteção de Dados. É composto por cinco diretores/as, incluindo o Diretor/a-Presidente/a, escolhidos/as e nomeados/as pelo Presidente da República, após aprovação pelo Senado Federal. Os/As diretores/as devem ser escolhidos entre brasileiros/as que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os/as quais serão nomeados/as.



O mandato no Conselho Diretor é de quatro anos e os/as membros/as apenas perdem os cargos quando houver renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar (**Artigo 55-E da Lei 13.709/2018**).

Já o **Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD)** é um órgão consultivo formado por 23 representantes de órgãos públicos, da sociedade civil, da comunidade científica, do setor produtivo e empresarial e do setor laboral.

O Conselho é composto pelos seguintes órgãos e entidades (**Artigo 58-A da Lei 13.709/2018**):

- 5 do Poder Executivo Federal;
- 1 do Senado Federal;
- 1 da Câmara dos Deputados;
- 1 do Conselho Nacional de Justiça;
- 1 do Conselho Nacional do Ministério Público;
- 1 do Comitê gestor da Internet do Brasil;
- 3 de entidades da sociedade civil com atuação relacionada à proteção de dados pessoais;
- 3 de instituições científicas, tecnológicas e de inovação;
- 3 de confederações sindicais representativas das categorias econômicas do setor produtivo;
- 2 de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais;
- 2 de entidades representativas do setor laboral.

Os/As membros/as do Conselho e respectivos suplentes são designados pelo Presidente da República. Os órgãos do poder público e o Comitê Gestor da Internet do Brasil devem fazer suas indicações ao Ministro de Estado Chefe da Casa Civil e as demais indicações podem ser livremente apresentadas para o Conselho Diretor da autoridade nacional, a partir da publicação de edital.

Após receber as indicações, o Conselho Diretor deve formar uma lista tríplice de titulares e suplentes para as vagas e encaminhar para o Ministro de Estado Chefe da Casa Civil, para escolha e nomeação do Presidente da República (**Artigo 58-A da Lei 13.709/2018**).



As principais competências do Conselho Nacional de Proteção de Dados Pessoais estão previstas no **artigo 58-B da Lei 13.709/2018**, sendo elas:

- **Propor diretrizes estratégicas** e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
- **Elaborar relatórios anuais de avaliação** da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- **Sugerir ações** a serem realizadas pela ANPD;
- **Elaborar estudos** e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade;
- **Disseminar o conhecimento** sobre a proteção de dados pessoais e da privacidade da população.

Qual a competência da Autoridade Nacional de Proteção de Dados (ANPD)?

De maneira geral, a Autoridade Nacional de Proteção de Dados tem a competência de assegurar a aplicação da Lei Geral de Proteção de Dados, garantindo a proteção aos direitos fundamentais da liberdade, da privacidade e da personalidade.

O **artigo 55-J da Lei 13.709/2018** estabelece as competências da autoridade nacional. Destacamos aqui as principais:

- ↗ Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (**Artigo 55-J, III da Lei 13.709/2018**);
- ↗ Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso (**Artigo 55-J, IV da Lei 13.709/2018**);
- ↗ Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança (**Artigo 55-J, VI da Lei 13.709/2018**);



- **Estimular a adoção** de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis (Artigo 55-J, VIII da Lei 13.709/2018);
- **Promover ações** de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional (Artigo 55-J, IX da Lei 13.709/2018);
- **Editar regulamentos e procedimentos** sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na Lei Geral de Proteção de Dados (Artigo 55-J, XIII da Lei 13.709/2018);
- **Ouvir** os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento (Artigo 55-J, XIV da Lei 13.709/2018);
- **Editar normas, orientações e procedimentos** simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclararem startups ou empresas de inovação, possam adequar-se à Lei (Artigo 55-J, XVIII da Lei 13.709/2018);
- **Deliberar**, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos (Artigo 55-J, XX da Lei 13.709/2018);
- **Articular-se com as autoridades reguladoras públicas** para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação (Artigo 55-J, XXIII da Lei 13.709/2018);
- **Implementar mecanismos** simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD (Artigo 55-J, XXIV da Lei 13.709/2018).



Como se dá a participação popular na Autoridade Nacional de Proteção de Dados?

A participação da sociedade civil se dá de forma representativa no **Conselho Nacional de Proteção de Dados Pessoais** e também por meio de consultas e audiências públicas. Lembrando que os regulamentos e normas editadas pela autoridade nacional devem seguir tais procedimentos de participação popular (**Artigo 55-J, § 2º da Lei 13.709/2018**).

As Organizações da Sociedade Civil e outras pessoas jurídicas ou físicas que realizem atividades de tratamento de dados pessoais devem transferir para a autoridade nacional seus bancos de dados?

Não. A lei não exige que as pessoas jurídicas ou físicas que façam tratamento de dados transfiram seus bancos de dados para a **Autoridade Nacional de Proteção de Dados**.

Como são aplicadas as sanções da Lei Geral de Proteção de Dados?

A aplicação das sanções são feitas a partir de uma criteriosa apreciação e ponderação das circunstâncias. Considera-se: **a gravidade do dano causado; qual a natureza das infrações e dos direitos pessoais afetados; a condição econômica do/a responsável; a adoção de políticas de boas práticas e governança; a pronta adoção de medidas corretivas; a boa fé do/a infrator/a; a reincidência; o princípio da proporcionalidade.** Como previsto no **artigo 50, § 1º da Lei Geral de Proteção de Dados**.

É responsabilidade da Autoridade Nacional de Proteção de Dados **aplicar as sanções administrativas** aos/às controladores/as e encarregados/as que cometam infrações. Para aplicação das sanções, é aberto um procedimento administrativo que possibilite a ampla defesa e, no final do processo, pode-se aplicar as seguintes sanções previstas no **artigo 52 da Lei Geral de Proteção de Dados**:



Advertência, com indicação de prazo para adoção de medidas corretivas (**Artigo 52,I da Lei 13.709/2018**);



Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício,



excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração (Artigo 52,II da Lei 13.709/2018);

- **Multa diária**, observando o limite total a que se refere o item anterior (Artigo 52,III da Lei 13.709/2018);
- **Publicização da infração** após devidamente apurada e confirmada a sua ocorrência (Artigo 52,IV da Lei 13.709/2018);
- **Bloqueio** dos dados pessoais a que se refere a infração até a sua regularização (Artigo 52,V da Lei 13.709/2018);
- **Eliminação** dos dados pessoais a que se refere a infração (Artigo 52,VI da Lei 13.709/2018);
- **Suspensão parcial** do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo/a controlador/a (Artigo 52,X da Lei 13.709/2018);
- **Suspensão do exercício** da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período (Artigo 52,XI da Lei 13.709/2018);
- **Proibição** parcial ou total do exercício de atividades relacionadas a tratamento de dados (Artigo 52,XII da Lei 13.709/2018).

A **Lei Geral de Proteção de Dados** também determina que a autoridade nacional deve editar um regulamento próprio com as metodologias que irão orientar o cálculo do valor-base das sanções de multa de acordo com os critérios da legislação.

Vale destacar que a quebra das regras em relação ao tratamento pessoal de dados não implica em uma multa imediata. As sanções são feitas de maneira gradativa, sendo que há outras penalidades mais leves que são aplicadas. Em relação à multa, ela é fixada a partir do porte e condições econômicas da instituição. Em relação às Organizações da Sociedade Civil, não há uma especificação na legislação, o que ainda deve ser regulamentado.



Qual o tratamento que se deve ter com os documentos físicos?

Como dito anteriormente, a **Lei Geral de Proteção de Dados** não faz distinção entre os documentos mantidos por meios digitais e físicos. Desta forma, tudo aquilo que diz respeito ao tratamento de dados também se aplica aos documentos físicos. A coleta, armazenamento e tratamento dos documentos físicos também devem seguir os requisitos exigidos pela legislação.

Para se adequar, é importante que as Organizações da Sociedade Civil, ao fazerem o mapeamento do fluxo de dados, também considerem os seus arquivos físicos. Será importante organizá-los para que sejam encontrados rapidamente de forma que permita um sistema eficiente de rastreamento. Outra questão é a eliminação destes documentos, as organizações devem adotar um procedimento. Lembrando que não devem ser guardados documentos físicos que não cumpram uma finalidade do controlador/a ou que sejam desnecessários.

Como deve ser feito o tratamento de dados pessoais de trabalhadores/as das Organizações da Sociedade Civil? Qual o prazo que se deve manter o tratamento destes dados?

Como dito, a legislação não estabelece um prazo específico de duração para o tratamento de dados pessoais, isso depende da finalidade. Em relação aos/às trabalhadores/as, diversos dados e documentos são exigidos pela própria legislação trabalhista por serem necessários para o pagamento da folha de pagamento e contribuições sociais. As OSCs devem estabelecer uma política de tratamento para estes dados e, quando a relação de trabalho termina, pode guardar esses dados por um período de tempo por segurança jurídica para eventuais processos trabalhistas e depois eliminá-los. No momento da contratação, é importante o consentimento dos/as trabalhadores/as sobre o tratamento de dados e período de duração. Ademais, as organizações devem ter uma política de proteção de tratamento de dados pessoais de trabalhadores/as que deve conter:

Os tipos de dados coletados em processos Seletivos e no momento da contratação;

Apresentação dos direitos dos/as trabalhadores/as Em relação aos seus dados;

Período de armazenamento dos dados coletados;

Explicação sobre o monitoramento como ponto biométrico, câmeras de vídeo, navegação de internet ou telefone;

Entre outras informações pertinentes.



As Organizações da Sociedade Civil podem solicitar antecedentes criminais de seus/suas trabalhadores/as?

Não. A **Lei 9.029/1995** proíbe que sejam exigidos documentos no momento da contratação que gerem alguma prática discriminatória. Em relação aos antecedentes criminais, o Tribunal Superior do Trabalho decidiu que este documento só pode ser exigido em casos específicos para determinadas profissões e devem ser esclarecidos os fins e as razões do pedido, como para as posições de motorista, trabalhadores/as que atuam com substâncias tóxicas ou com informações sigilosas, entre outras.

Ademais, a eventual existência de registro em certidão de antecedentes criminais não pode, por si só, ser fator impeditivo para a recolocação das pessoas egressas do sistema prisional no mercado de trabalho se a sua antiga condenação não guarda alguma relação com a atividade laboral.

Assim, essa determinação, apesar de não estar prevista na Lei Geral de Proteção de Dados, está de acordo com o princípio da finalidade. As Organizações da Sociedade Civil só podem exigir documentação no momento da contratação a partir do tipo de vaga a ser preenchida, qualificações necessárias para o cargo, necessidades específicas da organização ou mesmo para pagamento de direitos trabalhistas ou contribuições. Dessa forma, deve-se seguir os princípios da finalidade e necessidade, além de fazer o tratamento destes dados pessoais dos/as trabalhadores/as e/ou candidatos/as à vaga de acordo com a legislação.

Como deve ser feito o tratamento de dados de documentos contábeis?

O setor ou os/as responsáveis pelos documentos contábeis e financeiros da OSC também devem se adequar à Lei Geral de Proteção de Dados, uma vez que lidam com documentos pessoais como dados bancários, exames ocupacionais, além dos dados de identificação pessoal, ou seja, inúmeras informações que precisam de proteção. As Organizações da Sociedade Civil precisam desenvolver políticas internas de proteção e armazenamento destes dados. Pela legislação tributária, os documentos fiscais devem ser guardados pelo período mínimo de 5 anos.



É necessário ter alguma política específica para os cookies no website de acordo com a Lei Geral de Proteção de Dados?

Sim, todos os websites que utilizam cookies precisam ter uma política de acordo com a legislação.

Em primeiro lugar, é importante explicar o que são os cookies.

Quando uma pessoa acessa um website, este envia um arquivo de texto para o navegador utilizado. O arquivo armazena os dados do histórico de navegação como preferências, localização, identificação, entre outros. São os cookies que permitem que as senhas e logins fiquem salvos, por exemplo.

Em segundo, há outra informação relevante: nem todos os cookies carregam dados pessoais. Há diversos tipos de cookies que podem cumprir finalidades diferentes. Por exemplo, há cookies que são essenciais para viabilizar o funcionamento adequado do site, outros que informam como os/as visitantes interagem, o tempo de visita, quais áreas mais acessadas ou quaisquer problemas encontrados.

Para se adequar à política dos cookies no site é necessário entender, junto aos/as profissionais de tecnologia da informação, quais são os tipos de cookies que o site da organização utiliza. Nos casos em que forem usados cookies que não coletam e armazenam dados pessoais, é necessário criar um texto simples com a informação de que a organização utiliza cookies, o que é rastreado e qual a finalidade. Esta é uma exigência mínima adequada à Lei Geral de Proteção de Dados. Já nos casos em que o site dispara cookies que processam dados pessoais ou dados que, cruzados, podem identificar uma pessoa individualmente, é necessário, além do texto informando a utilização dos cookies, o consentimento do/a titular e a adequação de todo o processamento desses dados à nova lei.

É essencial entender por que os cookies estão sendo utilizados e qual a finalidade que a Organização da Sociedade Civil tem com este rastreamento. A política sobre os cookies deve estar, ainda, na Política de Privacidade da Organização da Sociedade Civil. Além disso, recomenda-se que, quando possível, faça-se investimento em tecnologias que permitam o/a titular desativar os cookies para acessar o website.

Como Adequar as
Organizações da Sociedade
Civil à **Lei Geral de Proteção**
de Dados





Como já explicado anteriormente, a importância das Organizações se adequarem à Lei Geral de Proteção de Dados tem a ver não apenas com uma exigência da legislação, mas também com a contribuição para uma cultura de proteção de dados e defesa de direitos fundamentais da liberdade e privacidade. Por isso, o comprometimento das Organizações da Sociedade Civil com a proteção de dados não pode ser algo apenas mecânico mas sim ser incorporado ao cotidiano como um compromisso com a privacidade das pessoas que se relacionam de alguma forma com a organização.

É relevante destacar que cada processo de adequação é único e vai depender das necessidades específicas de cada organização, a partir do tipo de dados pessoais coletados e armazenados, volume de dados, tamanho da equipe, entre outros fatores. O tempo de adequação também é variado de acordo com estes mesmos fatores.

O primeiro passo para a adequação é desenvolver uma reflexão dentro da OSC em relação à importância da Lei Geral de Proteção de Dados: os motivos que levam à adequação e quais os principais objetivos a serem alcançados. Cada organização terá um foco específico a partir das suas atividades e necessidades. É preciso também tomar uma decisão sobre a adequação: **quem será responsável por fazê-la?** As OSCs podem contratar consultoria, advogados/as ou prestadores de serviço para tal ou então realizá-la a partir da própria equipe, lembrando que existem cursos e treinamentos gratuitos e pagos online, além de diversos materiais que podem auxiliar neste processo. Vale destacar que grande parte dos procedimentos para seguir a Lei Geral de Proteção de Dados é simples, como a informação aos/às titulares de dados ou criação de um canal de contato etc. Para algumas medidas de segurança, pode ser necessário também o auxílio profissional de um técnico da informação que possa implementar softwares de proteção, tratar dos cookies no site etc.

O segundo passo é a conscientização e capacitação da equipe e dos órgãos diretivos sobre a Lei Geral de Proteção de Dados. Apesar da OSC ser obrigada a indicar um/a encarregado/a no tratamento de dados pessoais, é essencial que toda a equipe conheça os principais conceitos da Lei, como os direitos dos/as titulares, consentimento, finalidades da coleta e tratamento de dados, entre outros. Isso porque sabemos que, no cotidiano das organizações, é comum que diferentes pessoas da equipe façam alguma forma de tratamento de dados durante o desenvolvimento de suas atividades, assim, essa é uma forma de contribuir com a cultura de proteção de dados. A capacitação da equipe não é um processo que se encerra em apenas uma conversa.

Durante a adequação do tratamento de dados, é necessário um diálogo constante para que a equipe esteja ciente e conheça os procedimentos



internos, a política de proteção de dados adotada pela OCS, quem é o/a encarregado/a, entre outras informações relevantes. E essas informações vão estar mais evidentes apenas ao final do processo de adequação. Lembrando que a capacitação do/a encarregado/a de dados deve ser mais profunda e específica, já que será este/a o/a responsável por atender os/as titulares, tomar medidas em situações de risco de incidente de segurança, além de outras funções.

O terceiro passo é a análise em relação ao fluxo de dados da organização, isto é, entender como se dá todo o procedimento desde a coleta de dados até a sua exclusão. O recomendado é a identificação detalhada do tratamento: **como se dá a coleta de dados em cada área ou projeto de atuação (ou seja, por quais meios os dados pessoais entram em sua instituição); para qual finalidade ela é feita; quais as características desses dados (se são sensíveis ou não); como são armazenados; quais os métodos de proteção utilizados; e, por fim, como são descartados.** É a partir deste mapeamento que serão identificados todos os ajustes necessários para a adequação na governança dos dados. Para realizar o levantamento, pode ser feito um formulário digital, para que toda a equipe ou pessoas envolvidas no tratamento de dados preencha, ou uma escuta a partir de conversas.

O quarto passo é a governança sobre o tratamento de dados. Após o mapeamento do fluxo de dados, é necessário melhorar o tratamento de dados corrigindo as lacunas encontradas e procedimentos inadequados. Aqui se inclui a revisão da política de privacidade – ou adoção de uma, caso a OSC não possua –, a aprimoração de mecanismos para rastrear os dados tratados (saber quando foram coletados, para qual finalidade e por quanto tempo) e a adesão de um procedimento interno de proteção de dados.

Um ponto importante é identificar os dados que são coletados de forma desnecessária. No cotidiano das OSCs, às vezes é comum coletar dados como nome, CPF, endereço, mas sem uma real reflexão sobre a necessidade e finalidade desta coleta. Por exemplo, nos formulários digitais de inscrição para uma atividade virtual, **há a necessidade de saber o endereço ou estado civil da pessoa? Por quê?** Já um dado sensível, como o de orientação sexual, pode ser justificado por uma política de diversidade da organização ou para levantar estatísticas sobre a participação, mas tais finalidades devem ficar explícitas e dados desnecessários não devem ser coletados. A partir da definição do tempo de armazenamento, será feita a exclusão de dados que ultrapassaram este prazo, inclusive dados físicos mantidos sem real necessidade.

O mapeamento feito no passo anterior irá permitir definir as justificativas legais para captação e tratamento de dados das atividades das Organizações da Sociedade Civil. As justificativas devem estar documentadas, já que é direito dos/as titulares acessá-las. Quando possível, os dados devem ser anonimizados, ou seja, não se permitindo a identificação dos/as titulares. Como ajuste, recomenda-se a redação



de documentos de proteção de dados. Não há uma regra de documentos obrigatórios e isso vai depender das opções feitas por cada OSC no processo de adequação. O mais recomendado é que, no mínimo, as Organizações da Sociedade Civil tenham os seguintes documentos com modelos anexados:

Política de Privacidade: o documento divulgado no site com o nome e contato do/a encarregado/a, forma de coleta de dados, finalidades, mecanismos de proteção, se há compartilhamento de dados, período de armazenamento, direitos dos/as titulares, entre outros;

Política Interna de Tratamento e Proteção de Dados: orientações para os/as trabalhadores/as e dirigentes sobre os procedimentos de tratamento de dados adotados pela instituição;

Política de Tratamento de Dados Pessoais de Trabalhadores/as: documento para informar a política de tratamento de dados pessoais de trabalhadores/as, no momento da contratação, expondo as justificativas legais e procedimentos adotados;

Termo de Consentimento de Tratamento de Dados Pessoais: documento que registra a manifestação livre, informada e inequívoca pela qual o/a titular concorda com o tratamento de seus dados pessoais para finalidade específica, em conformidade com a **Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais**;

Textos para formulários ou outras formas de coleta de dados informando a finalidade e política de tratamento de dados, além dos direitos dos/as titulares;

Aviso de Cookies (rastreadores): nos casos em que o site da OSC utilize cookies, é necessário um texto simples com esta informação e finalidade do rastreamento.

O quinto passo diz respeito à segurança da informação. É a utilização de mecanismos que assegurem a proteção do banco de dados mantido pela organização, a partir de software e outros meios. No processo de mapeamento de fluxos, podem ser identificadas vulnerabilidades em relação à proteção de dados que também devem ser consideradas e corrigidas. Para a efetivação deste passo, o mais provável é a necessidade de contratação de um profissional de tecnologia da informação, caso a organização não tenha já um/a prestador/a de serviço. Há alguns coletivos e instituições que prestam serviços de forma gratuita.



O sexto passo é a definição do/a encarregado/a pelo tratamento de dados. Essa é uma decisão a ser tomada pelo órgão diretivo da OSC responsável pela tomada de decisões, que pela legislação é chamado/a de controlador/a. Já o/a encarregado/a será aquele/a responsável pelas atividades de tratamento de dados pessoais, o que inclui o contato com a Autoridade Nacional de Proteção de Dados (ANPD) e com os/as titulares. O/a encarregado/a não precisa ter uma profissão específica, como advogado/a ou profissional da tecnologia, o determinante é ser uma pessoa que conheça a Lei Geral de Proteção de Dados e saiba operar mecanismos de proteção de dados.

O sétimo passo é a criação de um procedimento de atendimento aos/às titulares de dados pessoais ou qualquer pessoa que requeira informação sobre o tratamento de dados, pode ser um e-mail ou telefone específico ou o contato do/a próprio/a encarregado/a.

Por fim, após o processo de adequação, recomenda-se um monitoramento e avaliação constantes sobre o tratamento de dados da OSC. É uma forma permanente de analisar se a adequação e a proteção de dados estão funcionando. Além disso, podem surgir dúvidas ou mesmo situações inusitadas posteriores ao processo. Para isso, um mecanismo é a adoção de listas de condutas (checklists) para que a equipe faça uma avaliação sobre a Política de Proteção de Dados. Outro ponto é haver um acompanhamento e diálogo entre o/a controlador/e e encarregado/a.

Destaca-se que todos esses passos e recomendações não precisam ser realizados nessa ordem, sendo esta apenas uma sugestão de organização. Os procedimentos podem ocorrer de forma concomitante ou mesmo em outra ordem, pois, como dito, cada processo de adequação é único e vai depender das características e atividades de cada organização.

MODELO DE TEXTO SIMPLES PARA FORMULÁRIOS OU OUTRAS FORMAS DE COLETA DE DADOS

AUTORIZAÇÃO: Conforme **Lei Geral de Proteção dos Dados (Lei 13.709/2018)**, a signatária desta solicitação autoriza que os dados acima informados sejam utilizados apenas para fins **[especificar os fins]**. A guarda e armazenamento destas informações são de responsabilidade do **[Controlador/a]**.



orientação jurídica.

ANEXO I - Modelo de termo de consentimento
de tratamento de dados pessoais





➤ ANEXO I - Modelo de termo de consentimento de tratamento de dados pessoais

[Termo de Consentimento para Armazenamento e Tratamento de Dados Pessoais em Conformidade com a LGPD]

Este documento visa registrar a manifestação livre, informada e inequívoca pela qual o/a titular concorda com o tratamento de seus dados pessoais para finalidade específica, em conformidade com a **Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD)**.

Informamos que coletamos os dados [descrição dos dados] para fins [descrição dos fins].

O/A Controlador/a [Nome da organização da sociedade civil] poderá manter e tratar os dados pessoais do/a titular durante todo o período em que os mesmos forem pertinentes ao alcance das finalidades listadas no presente termo, sendo que os dados pessoais anonimizados, sem possibilidade de associação ao/à titular, poderão ser mantidos por período indefinido.

Você poderá, a qualquer momento:

- Confirmar a existência de tratamento de dados, de maneira simplificada ou em formato claro e completo;
- Acessar seus dados, podendo solicitá-los em uma cópia legível sob forma impressa ou por meio eletrônico, seguro e idôneo;
- Corrigir seus dados, ao solicitar a edição, correção ou atualização dos mesmos;
- Limitar seus dados quando desnecessários, excessivos ou tratados em desconformidade com a legislação por meio da anonimização, bloqueio ou eliminação;
- Solicitar a portabilidade de seus dados por meio de um relatório de dados cadastrais que o/a [Nome da organização da sociedade civil] trata a respeito;
- Eliminar seus dados tratados a partir de seu consentimento, exceto nos casos previstos em lei;
- Revogar seu consentimento, desautorizando o tratamento de seus dados;
- Informar-se sobre a possibilidade de não fornecer seu consentimento e sobre as consequências de negativa.

As solicitações e questionamentos acerca do tratamento e eliminação de seus dados deverão ser realizadas por meio do [e-mail ou telefone da OSC].



➤ ANEXO I - Modelo de termo de consentimento de tratamento de dados pessoais

[Link para a Política de Proteção de Dados da Organização da Sociedade Civil]

Consentimento por meio virtual:

Caso **ACEITE** que seus Dados Pessoais sejam coletados, por favor, concorde com este aviso.

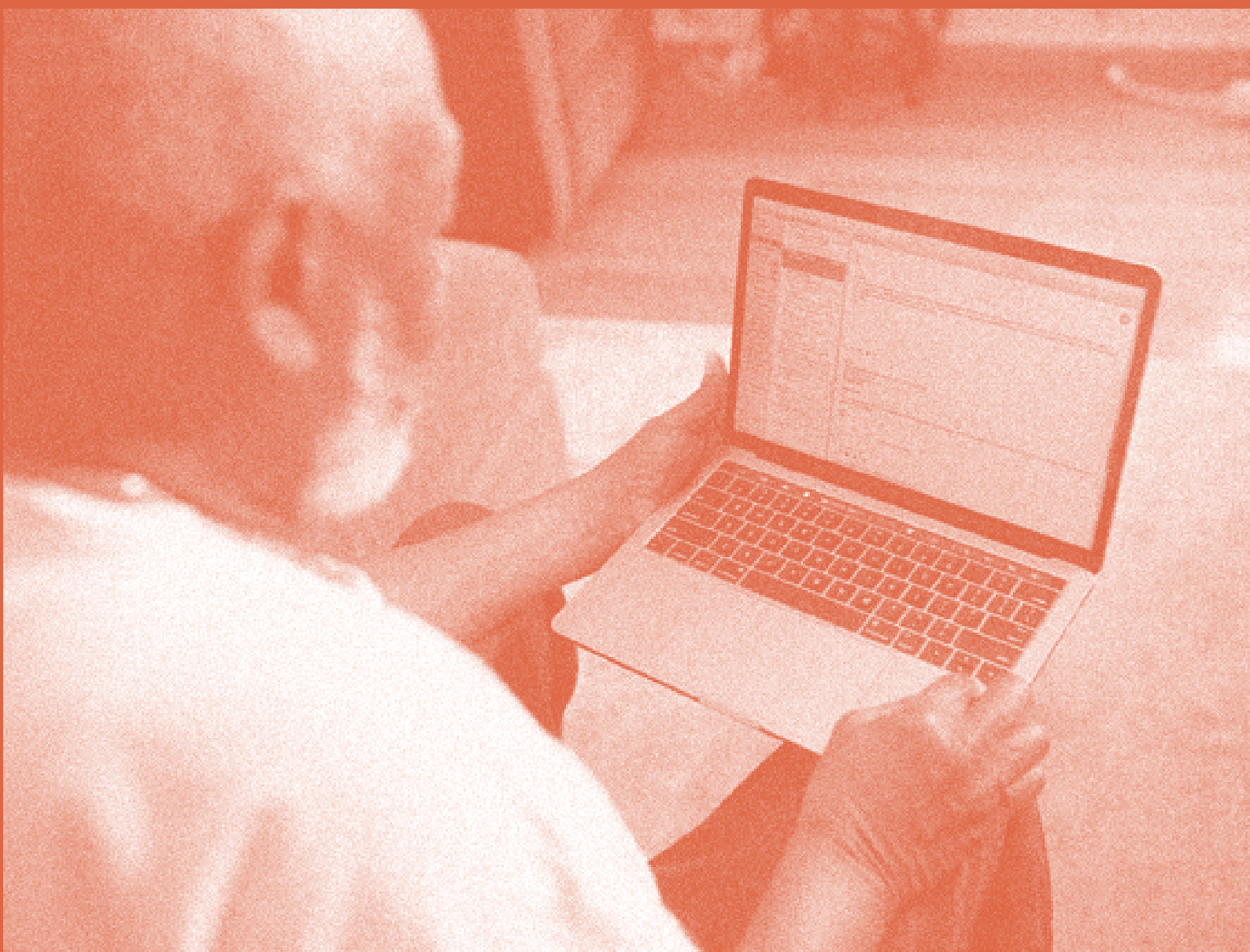
- A) CONCORDO []
B) NÃO CONCORDO []

Consentimento via documento físico:

-
- Assinatura do responsável**
[Data]
[Nome completo]
[RG]

orientação jurídica.

ANEXO II - Modelo de política de proteção e tratamento de dados pessoais de trabalhadores/as





➔ ANEXO II - Modelo de política de proteção e tratamento de dados pessoais de trabalhadores/as

[Política de Proteção Tratamento de Dados Pessoais de Trabalhadores/as]*

* Documento para informar a política de tratamento de dados pessoais de trabalhadores/as, no momento da contratação, expondo as justificativas legais exigidas no Estatuto.

O/A [Nome da organização da sociedade civil] defende os direitos e liberdades civis e, por isso, está comprometido/a em promover níveis adequados de segurança para assegurar a privacidade e proteger os dados pessoais de seus/suas trabalhadores/as.

Este documento estabelece como é feita a coleta, uso e transparência de informações dos trabalhadores/as que estabeleçam algum tipo de relação de trabalho por tempo determinado ou indeterminado com a [Nome da organização da sociedade civil].

Desta forma, a/o [Nome da organização da sociedade civil] inscrita no CNPJ/MF sob o nº [CNPJ] no papel de Controlador/a de dados, obriga-se ao disposto na presente Política de tratamento de dados pessoais de trabalhadores/as.

Para os processos coletivos, coletamos dados dos/as candidatos/as com a finalidade de conhecer melhor o perfil e estabelecer a melhor escolha. Os tipos de dados coletados irão depender das características exigidas para a vaga, sendo que a instituição se compromete a coletar o mínimo necessário para esta finalidade. Pode-se coletar dados pessoais sensíveis com o objetivo de implementar políticas de inclusão e diversidade na equipe. Após o processo seletivo, o/a [Nome da organização da sociedade civil] irá guardar os dados pelo período de [tempo] e depois irá eliminá-los de seu banco de dados.

No momento da contratação, coletamos os seguintes dados dos/as trabalhadores/as:

1. **Dados tratados por obrigação legal:** [Descrição dos dados];
2. **Dados tratados por legítimo interesse do/a controlador/a:** [Descrição dos dados].

Os dados dos/as trabalhadores/as da [Nome da organização da sociedade civil] são armazenados pelo período de [tempo] após o encerramento da relação trabalhista. Após este período, os dados são eliminados do banco de dados da organização, sendo que os dados pessoais anonimizados, sem possibilidade de associação ao/à titular, poderão ser mantidos por período indefinido.



➔ ANEXO II - Modelo de política de proteção e tratamento de dados pessoais de trabalhadores/as

São direitos de todos os/as trabalhadores enquanto titulares de dados pessoais:

- Confirmar a existência de tratamento de dados, de maneira simplificada ou em formato claro e completo;
- Acessar seus dados, podendo solicitá-los em uma cópia legível sob forma impressa ou por meio eletrônico, seguro e idôneo;
- Corrigir seus dados, ao solicitar a edição, correção ou atualização dos mesmos;
- Limitar seus dados quando desnecessários, excessivos ou tratados em desconformidade com a legislação por meio da anonimização, bloqueio ou eliminação;
- Solicitar a portabilidade de seus dados por meio de um relatório de dados cadastrais que o/a [Nome da organização da sociedade civil] trata a respeito;
- Eliminar seus dados tratados a partir de seu consentimento, exceto nos casos previstos em lei;
- Revogar seu consentimento, desautorizando o tratamento de seus dados;
- Informar-se sobre a possibilidade de não fornecer seu consentimento e sobre as consequências de negativa.

* Opcional. para casos em que a organização compartilhe dados com parceiros:

A natureza das atividades realizadas pelo/a [Nome da organização da sociedade civil], em regra, envolve cooperação com outras organizações da sociedade civil, órgãos públicos ou plataformas de gestão, o que pode ocasionar o compartilhamento de informações.

No entanto, caso haja necessidade de compartilhamento de dados pessoais, isso somente ocorrerá após informe aos/às trabalhadores/as. O compartilhamento será limitado ao mínimo adequado e necessário para o cumprimento de alguma das finalidades específicas e previamente informadas. E, quando isso ocorrer, incorporamos aos instrumentos contratuais cláusulas de responsabilidade para assegurar que qualquer terceiro que receba os dados garanta a eles a proteção adequada e preserve a privacidade. Não compartilhamos dados pessoais com nenhum/a terceiro/a não autorizado/a.



➤ ANEXO II - Modelo de política de proteção e tratamento de dados pessoais de trabalhadores/as

A seguir, você encontra a lista de terceiros/as envolvidos/as na coleta, tratamento e compartilhamento de dados pessoais sob responsabilidade do/a [Nome da organização da sociedade civil]:

[Lista de terceiros/as]

* **Opcional.** para situações em que a organização tenha uma política de monitoramento: O/A [Nome da organização da sociedade civil] adota os seguintes métodos de monitoramento de seus/suas trabalhadores/as: [Descrição dos métodos]*.

* **Exemplos:** ponto biométrico; câmeras de vídeos; serviços de monitoramento dos/as trabalhadores/as na internet e uso de telefone.

[Data da última atualização]
[Nome da Organização da Sociedade Civil]

orientação jurídica.

ANEXO III - Modelo de texto informando a
coleta de dados pessoais





➤ ANEXO III - Modelo de texto informando a coleta de dados pessoais

* Texto para formulários ou outras formas de coleta de dados.

Informamos que esta coleta de dados é destinada à finalidade específica, em conformidade com a **Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)**. Coletamos os dados pessoais **[Dados - Nome, Telefone, E-mail, Endereço]** para fins de **[especificar a finalidade: transmitir mensagens, enviar documentos, coleta, classificação, utilização, acesso, comunicação, arquivamento e armazenamento]**. Os seus dados pessoais serão armazenados e preservados por um período indeterminado; os dados são registrados e armazenados no sistema.

Você poderá, **a qualquer momento**:

- Ter acesso às informações sobre a forma e a duração de tratamento dos seus dados; Solicitar a atualização ou correção dos seus dados;
- Solicitar a eliminação dos seus dados pessoais tratados e revogação do consentimento, nos termos da Lei. A partir da solicitação, os dados são eliminados da plataforma virtual.

O/A Controlador/a poderá manter e tratar os dados pessoais do/a Titular durante todo o período em que os mesmos forem pertinentes ao alcance das finalidades listadas no presente termo, sendo que os dados pessoais anonimizados, sem possibilidade de associação ao/à Titular, poderão ser mantidos por período indefinido.

As solicitações e questionamentos acerca do tratamento e eliminação de seus dados deverão ser realizadas por meio do **[e-mail ou do telefone]** .

[Link para a Política de Proteção de Dados da Organização da Sociedade Civil]

orientação jurídica.

ANEXO IV - Modelo de política de privacidade





➤ ANEXO IV - Modelo de política de privacidade

[Política de Privacidade]

O/A **[Nome da organização da sociedade civil]** defende os direitos e liberdades civis e, por isso, está comprometido/a em promover níveis adequados de segurança online para assegurar a sua privacidade e proteger os seus dados pessoais.

Esta Política de Privacidade estabelece como é feita a coleta, uso e transparência de informações de qualquer pessoa que tenha algum tipo de relação com a nossa organização e outras pessoas que acessem ou usem nosso site. O objetivo é conferir transparência às práticas relacionadas ao nosso sítio eletrônico para que você tenha confiança em nosso compromisso e adequação à **Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018)** e às demais normas do ordenamento jurídico brasileiro aplicáveis.

Desta forma, a/o **[Nome da organização da sociedade civil]** inscrita no CNPJ/MF sob o nº **[CNPJ]** no papel de Controlador/a de dados, obriga-se ao disposto na presente Política de Privacidade.

Eventualmente, esta Política poderá passar por ajustes e revisões no intuito de melhor corresponder ao compromisso de proteger seus dados. Por isso, manteremos a data da última atualização ao final do documento e recomendamos que você verifique periodicamente.

a) Quais dados coletamos?

É importante que você saiba que o website coleta automaticamente atributos associados aos seus dispositivos eletrônicos, tais como: provedor de acesso, sistema operacional, navegador, configurações de vídeo (tamanho/resolução e quantidade de cores), data e hora do acesso, cidade e país do acesso. Essa é uma coleta padrão normalmente realizada por sites para gerar estatísticas de acesso.

Nosso website não coleta ou armazena seus dados pessoais sem que você os tenha disponibilizado voluntariamente, ou seja, não há coleta automática de informações como nome, data de nascimento, estado civil, profissão, raça, gênero, CPF, dados bancários, endereço residencial ou comercial, ou quaisquer outros que identifiquem você pessoalmente. Se alguma dessas informações for necessária para disponibilizarmos serviço, notícia ou produtos, solicitaremos que preencha um formulário ou cadastro de forma livre e esclarecida.



➤ ANEXO IV - Modelo de política de privacidade

A solicitação, coleta e armazenamento de dados pessoais pelo/a **[Nome da organização da sociedade civil]** deverá ser restrita ao mínimo suficiente para atender à sua demanda ou para corresponder ao nível de relacionamento que você possui com a nossa organização – interessado/a, parceiro/a, voluntário/a, participante de projeto, cursista, funcionário/a, apoiador/a, doador/a etc. Isso quer dizer que não existe uma única regra de quais dados são coletados, havendo um grau de variação em razão dos distintos níveis de relacionamento possíveis. Contudo, por outro lado, significa que não coletamos dados desnecessários e que os dados sensíveis serão solicitados com a devida justificativa.

b) Por quais meios coletamos seus dados pessoais?

As informações que coletamos a seu respeito podem ter nos sido fornecidas diretamente por você, por terceiros, coletadas de forma automática ou serem provenientes de bases públicas disponíveis online.

- Dados pessoais fornecidos pelo/a titular:

[Descrição dos meios]*

- Dados pessoais coletados automaticamente:

[Descrição dos meios]*

* Seguem abaixo alguns exemplos de textos, mas eles devem se adequar aos meios que a organização utiliza:

Dados pessoais fornecidos pelo/a titular:

“Em muitas de nossas atividades, poderemos solicitar que você preencha um formulário ou cadastro eletrônico, utilizando aplicativos.”

Obtidas por intermédio de outras plataformas:

“Em algumas circunstâncias, nosso site poderá redirecionar você para uma plataforma de gestão de inscrição e pagamento (Even3, PagSeguro, PayPal etc.), que operacionalizará a coleta de dados pessoais e os repassará ao/à **[Nome da organização da sociedade civil]**.”



➤ ANEXO IV - Modelo de política de privacidade

Automaticamente: “Em algumas situações, também poderemos coletar dados automaticamente dos dispositivos que você utiliza para acessar o nosso site ou aplicação mobile. Essas informações nos auxiliam a gerar estatísticas de acesso e, assim, conhecer melhor o público que os utiliza. Isso é importante para que possamos aperfeiçoá-los cada vez mais e adequá-los ao maior público possível. Alguns desses dados podem ser coletados por meio de cookies ou tecnologias similares.”

Disponíveis Publicamente: “Podemos também tratar informações que sejam de domínio público e que se encontrem em bancos de dados oficiais, incluindo, mas não se limitando a, mídias sociais (como o Facebook, Instagram, LinkedIn, Twitter etc.). Nesse caso, as informações só são coletadas caso você tenha permitido previamente, ficando assegurado o direito de revogar a permissão.”

c) Consentimento

É a partir do seu consentimento que tratamos os seus dados pessoais. O consentimento é a manifestação livre, informada e inequívoca pela qual você autoriza o/a **[Nome da organização da sociedade civil]** a tratar seus dados.

Assim, em consonância com a Lei Geral de Proteção de Dados, seus dados só serão coletados, tratados e armazenados mediante prévio e expresso consentimento.

O seu consentimento será obtido de forma específica para cada finalidade acima descrita, evidenciando o compromisso de transparência e boa-fé do/a **[Nome da organização da sociedade civil]** para com os/as titulares, seguindo as regulações legislativas pertinentes.

Ao fornecer seus dados pessoais, você está ciente e consentindo com as disposições desta Política de Privacidade, além de conhecer seus direitos e como exercê-los.

A qualquer tempo e sem nenhum custo, você poderá revogar o seu consentimento.



➤ ANEXO IV - Modelo de política de privacidade

d) Com quais finalidades armazenamos e utilizamos seus dados pessoais?

As informações pessoais coletadas pela/o **[Nome da organização da sociedade civil]** servem para diferentes propósitos a depender do seu nível de relacionamento com a organização.

A regra é que os dados sirvam tão somente para atender à finalidade para a qual eles nos foram fornecidos por você, ou para outras finalidades compatíveis e desde que informadas a você no momento da coleta de dados.

Com base no nosso legítimo interesse, também poderemos tratar os seus dados pessoais para viabilizar as atividades cotidianas do/a **[Nome da organização sociedade civil]**.

[Incluir outras finalidades].

e) Quais são os seus direitos?

O/A **[Nome da organização da sociedade civil]** assegura os direitos dos/as titulares de dados pessoais previstos no artigo 18 da Lei Geral de Proteção de Dados. Desta forma, você pode, de maneira gratuita e a qualquer tempo:

- Confirmar a existência de tratamento de dados, de maneira simplificada ou em formato claro e completo;
- Acessar seus dados, podendo solicitá-los em uma cópia legível sob forma impressa ou por meio eletrônico, seguro e idôneo;
- Corrigir seus dados, ao solicitar a edição, correção ou atualização dos mesmos;
- Limitar seus dados quando desnecessários, excessivos ou tratados em desconformidade com a legislação por meio da anonimização, bloqueio ou eliminação;
- Solicitar a portabilidade de seus dados por meio de um relatório de dados cadastrais que o/a **[Nome da organização da sociedade civil]** trata a respeito;
- Eliminar seus dados tratados a partir de seu consentimento, exceto nos casos previstos em lei;
- Revogar seu consentimento, desautorizando o tratamento de seus dados;
- Informar-se sobre a possibilidade de não fornecer seu consentimento e sobre as consequências de negativa.



➤ ANEXO IV - Modelo de política de privacidade

f) Como você pode exercer seus direitos de titular?

Para exercer seus direitos de titular, você deve entrar em contato com o/a **[Nome do/a encarregado/a]** por meio dos seguintes meios disponíveis:

[Meios de contato]

g) Como e por quanto tempo seus dados serão armazenados?

Seus dados pessoais coletados pelo/a **[Nome da organização da sociedade civil]** serão utilizados e armazenados durante o tempo necessário para que as finalidades elencadas no momento do consentimento sejam atingidas, considerando os direitos dos/as titulares dos dados e dos/as controladores/as.

Findado o período de armazenamento dos dados pessoais, estes serão excluídos de nossas bases de dados ou anonimizados, ressalvadas as hipóteses legalmente previstas no artigo 16 lei geral de proteção de dados, a saber:

- I – cumprimento de obrigação legal ou regulatória pelo controlador;
- II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Isto é, informações pessoais sobre você que sejam imprescindíveis para o cumprimento de determinações legais, judiciais e administrativas e/ou para o exercício do direito de defesa em processos judiciais e administrativos serão mantidas, a despeito da exclusão dos demais dados.

O armazenamento de dados coletados pelo/a **[Nome da organização da sociedade civil]** reflete o nosso compromisso com a segurança e privacidade dos seus dados. Empregamos medidas e soluções técnicas de proteção aptas a garantir a confidencialidade, integridade e inviolabilidade dos seus dados. Além disso, também contamos com medidas de segurança apropriadas aos riscos e com controle de acesso às informações armazenadas.



➤ ANEXO IV - Modelo de política de privacidade

h) O que fazemos para manter seus dados seguros?

Para mantermos suas informações pessoais seguras, utilizamos ferramentas físicas, eletrônicas e gerenciais orientadas para a proteção da sua privacidade.

Aplicamos essas ferramentas levando em consideração a natureza dos dados pessoais coletados, o contexto e a finalidade do tratamento. Entre as medidas que adotamos, destacamos as seguintes:

- [Descrição das medidas adotadas];
- [Descrição das medidas adotadas].

Buscamos aplicar protocolos internos que determinam como os dados pessoais devem ser tratados pela organização, definindo atribuições e responsabilidades. Essas normas têm como objetivo garantir o tratamento adequado e lícito dos dados pessoais que detemos, inclusive dos seus. Comprometemo-nos em adotar as melhores posturas para evitar incidentes de segurança. Contudo, é necessário destacar que nenhuma página virtual é inteiramente segura e livre de riscos. É possível que, apesar de todos os nossos protocolos de segurança, ocorram incidentes de segurança.

Em caso de incidentes de segurança que possam gerar risco ou dano relevante para você ou qualquer outro/a titular, comunicaremos aos afetados/as e à Autoridade Nacional de Proteção de Dados sobre o ocorrido, em consonância com as disposições da Lei Geral de Proteção de Dados.

i) Com quem seus dados podem ser compartilhados?

A natureza das atividades realizadas pelo/a [Nome da organização da sociedade civil], em regra, envolve cooperação com outras organizações da sociedade civil, órgãos públicos ou plataformas de gestão, o que pode ocasionar o compartilhamento de informações.

No entanto, caso haja necessidade de compartilhamento de dados pessoais, isso somente ocorrerá se você for informado/a e consentir. O compartilhamento será limitado ao mínimo adequado e necessário para o cumprimento de alguma das finalidades específicas e previamente informadas a você. E, quando isso ocorrer, incorporaremos aos instrumentos contratuais cláusulas de responsabilidade para assegurar que qualquer terceiro que receba os dados garanta a eles a proteção adequada e preserve a privacidade. Não compartilhamos dados pessoais com nenhum/a terceiro/a não autorizado/a.



➤ ANEXO IV - Modelo de política de privacidade

* Opcional. caso haja terceiros/as ou parceiros/as envolvidos/as no tratamento e compartilhamento de dados pessoais:

A seguir, você encontra a lista de terceiros/as envolvidos na coleta, tratamento e compartilhamento de dados pessoais sob responsabilidade do/a [Nome da organização da sociedade civil]:

[Lista dos nomes dos/as terceiros/as ou parceiros/as envolvidos/as].
Todavia, nossos parceiros/as têm suas próprias Políticas de Privacidade, que podem divergir desta. Recomendamos a leitura desses documentos, que você pode acessar aqui:

[Lista com links das Políticas de Privacidades dos/as parceiros/as envolvidos/as].

j) Cookies ou dados de navegação

O/A [Nome da organização da sociedade civil] faz uso de cookies, que são arquivos de textos que podem ser armazenados em seus dispositivos eletrônicos quando você visita um site na internet.

Ao acessar nosso site e consentir com o uso de cookies, você manifesta conhecer e aceitar a utilização de um sistema de coleta de dados de navegação com uso de cookies em seu dispositivo.

O/A [Nome da organização da sociedade civil] utiliza os seguintes cookies: [descrição dos tipos de cookies utilizados pelo site e a finalidade].

Você pode, a qualquer tempo e sem nenhum custo, alterar as permissões, bloquear ou recusar os cookies. Todavia, a revogação do consentimento de determinados cookies pode inviabilizar o funcionamento correto de alguns recursos da plataforma. Para gerenciar os cookies do seu navegador, basta fazê-lo diretamente nas configurações do navegador, na área de gestão de cookies.



➤ ANEXO IV - Modelo de política de privacidade

k) Alteração desta Política de Privacidade

A atual versão da Política de Privacidade foi formulada e atualizada pela última vez em: **[data da última atualização da Política de Privacidade]**.

Reservamos o direito de modificar essa Política de Privacidade a qualquer tempo, principalmente em função da adequação a eventuais alterações feitas em nosso site ou em âmbito legislativo. Recomendamos que você a revise com frequência.

Eventuais alterações entrarão em vigor a partir de sua publicação em nosso site e sempre o/a notificaremos acerca das mudanças ocorridas. Ao fornecer seus dados pessoais após tais modificações, você as consente.

l) Responsabilidade

O/A **[Nome da organização da sociedade civil]** prevê a responsabilidade dos/as agentes que atuam nos processos de tratamento de dados, em conformidade com os **artigos 42 a 45 da Lei Geral de Proteção de Dados**. Comprometemo-nos em manter esta Política de Privacidade atualizada, observando suas disposições e zelando por seu cumprimento.

Além disso, também assumimos o compromisso de buscar condições técnicas e organizativas seguramente aptas para proteger todo o processo de tratamento de dados.

Caso a Autoridade Nacional de Proteção de Dados exija a adoção de providências em relação ao tratamento de dados realizado pelo/a **[Nome da organização da sociedade civil]**, comprometemo-nos em segui-las. Destacamos que, em caso de incidentes de segurança que possam gerar risco ou dano relevante para você ou qualquer um/a de nossos usuários/as, comunicaremos aos/às afetados/as e à Autoridade Nacional de Proteção de Dados sobre o ocorrido e cumprimos as providências necessárias.

m) Encarregado/a de Proteção de Dados

O/A **[Nome da organização da sociedade civil]** disponibiliza os seguintes meios para que você possa entrar em contato conosco para exercer seus direitos de titular: **[meios de contato]**.

Caso tenha dúvidas sobre esta Política de Privacidade ou sobre os dados pessoais que tratamos, você pode entrar em contato com o/a nosso/a Encarregado/a de Proteção de Dados Pessoais por meio do seguinte contato:

- **[Nome do/a Encarregado/a]**
- **[CPF do/a Encarregado/a]**
- **[E-mail do/a Encarregado/a]**



➤ ANEXO IV - Modelo de política de privacidade

n) Definições

A fim de proporcionar maior clareza para você quanto ao conteúdo desta Política, as palavras e expressões, no singular ou no plural, foram utilizadas com os seguintes significados:

Titular: pessoa física a quem se referem os dados pessoais;

Controlador/a: termo que designa a quem compete as decisões referentes ao tratamento de dados pessoais, no nosso caso é **[Nome da organização da sociedade civil ou órgão diretivo responsável pelas decisões]**.

Encarregado/a: termo que designa a pessoa indicada pelo/a **[Nome da organização da sociedade civil]** para atuar como canal de comunicação entre nossa organização, você e a Autoridade Nacional de Proteção de Dados (ANPD).

Dados pessoais: qualquer informação que identifique ou que possa identificar uma pessoa física, como – por exemplo – um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;

Dados pessoais sensíveis: qualquer dado pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico;

Tratamento: coleta, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, atualização, comunicação, transferência, compartilhamento e extração de dados pessoais;

Anonimização: procedimento que quebra a ligação entre o/a titular de dados e as informações sobre ele/a, de forma que impeça a identificação da pessoa a partir dos dados pessoais

- **[Data da última atualização da Política de Privacidade]**
- **[Nome da Organização da Sociedade Civil]**

orientação jurídica.

ANEXO V - modelo de política
interna de proteção de dados





➔ ANEXO V - modelo de política interna de proteção de dados

* Este documento serve como referência para todos/as os/as trabalhadores/as da Organização, dirigentes estatutários ou não e outros profissionais que se relacionem com a organização. Deve conter orientações sobre a conduta adequada e adotada pela OSC para lidar com os dados pessoais.

O/A [Nome da organização da sociedade civil] defende os direitos e liberdades civis e, por isso, está comprometido/a em promover níveis adequados de segurança online para assegurar a sua privacidade e proteger seus dados pessoais.

Esta Política Interna de Proteção de Dados estabelece as orientações para toda a equipe (trabalhadores/as, prestadores de serviço e dirigentes estatutários ou não) de qual conduta adotar para a coleta, uso e transparência de informações de qualquer pessoa que tenha algum tipo de relação com a nossa organização e outras pessoas que acessem ou usem nosso site.

Desta forma, a/o [Nome da organização da sociedade civil] inscrita no CNPJ/MF sob o nº [CNPJ] no papel de Controlador/a de dados, obriga-se ao disposto na presente Política Interna de Proteção de Dados e todos/as os/as profissionais e dirigentes que tenham vínculo com a organização devem cumprir e se atentar às presentes orientações.

Os principais conceitos relacionados à Segurança da Informação são:

Titular: pessoa física a quem se referem os dados pessoais;

Controlador/a: termo que designa a quem compete as decisões referentes ao tratamento de dados pessoais, no nosso caso é [Nome da organização da sociedade civil ou órgão diretivo responsável pelas decisões];

Encarregado/a: termo que designa a pessoa indicada pelo/a [Nome da organização da sociedade civil] para atuar como canal de comunicação entre nossa organização, você e a Autoridade Nacional de Proteção de Dados (ANPD);

Dados pessoais: qualquer informação que identifique ou que possa identificar uma pessoa física, como – por exemplo – um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;

Dados pessoais sensíveis: qualquer dado pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico;

Tratamento: coleta, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, atualização, comunicação, transferência, compartilhamento e extração de dados pessoais;



➤ ANEXO V - modelo de política interna de proteção de dados

Anonimização: procedimento que quebra a ligação entre o/a titular de dados e as informações sobre ele/a, de forma que impeça a identificação da pessoa a partir dos dados pessoais;

Incidente de proteção de segurança: é todo acontecimento que pode comprometer a segurança de dados pessoais. O incidente pode levar a destruição, perda, alteração, divulgação, acesso não autorizado ou venda ilegal de dados pessoais. Pode ocorrer de forma acidental ou ilícita.

[Incluir outros conceitos pertinentes]

No/a [Nome da organização da sociedade civil], coletamos e fazemos o tratamento das seguintes informações pessoais, sendo que para cada uma há um nível de confidencialidade diferente: [Incluir quais tipo de informações são coletadas e como é classificada a sua confidencialidade].

- Para assegurar a proteção de dados pessoais, adotamos as seguintes medidas: [Descrição das medidas adotadas].
- Como provedor de armazenamento dos arquivos da instituição, utilizamos o: [Nome do provedor e outras especificações necessárias].
- Recomendamos que todos/as, ao utilizarem os computadores da organização e internet, adotem as seguintes medidas: [Descrição das recomendações] *Exemplos: restrição de sites, cuidados adotados no acesso a arquivos ou conteúdos, entre outras.

O Técnico de Informação do/a [Nome da organização da sociedade civil] responsável é [Nome] [Contato de e-mail ou telefone]. Sendo que todos/as podem contatá-lo/a caso necessitem de auxílio.



➤ ANEXO V - modelo de política interna de proteção de dados

[Política de Incidente de Segurança]

Apesar de tomarmos todas as medidas de segurança e adequação à Lei Geral de Proteção de Dados, sabemos que incidentes de segurança podem acontecer, por isso, definimos aqui quais procedimentos a serem adotados em caso de comprometimento ou violação de dados pessoais.

Em casos de incidente de segurança, devem ser responsáveis por lidar com a questão junto ao/à encarregado/a: **[Nomes dos/as responsáveis]***;

*** Opcional - quando a OSC possuir estes suportes:**

Quando necessário, serão consultados/as os/as:

Técnico da Informação: [Nome] [Contato]

Jurídico: [Nome] [Contato]

Orientamos todos/as os/as trabalhadores/as e dirigentes, quando perceberem uma falha que possa gerar um incidente de proteção de dados, a comunicarem imediatamente o/a encarregado/a: **[Nome] [Contato]**.

O/A encarregado/a e o/a responsável ou equipe responsável devem comunicar às pessoas que possam vir a sofrer algum dano a partir do incidente de proteção de dados e à Autoridade Nacional de Proteção de Dados, conforme previsão legal.

*** Opcional: [Incluir como a equipe deve avaliar a gravidade do incidente. Uma alternativa é a utilização de matriz de risco que classifica, a partir do contexto da sua organização, qual a gravidade do incidente.]**

[Última data de atualização]

[Nome da organização da sociedade civil]

cadernos Abong

Vínculos de Trabalho Não Remunerado
nas Organizações da Sociedade Civil,
**Helena Duarte, Henrique B. Frota
& Mauri Cruz. (1)**

Engajamento Político e Constituição
das Organizações da Sociedade Civil,
**Helena Duarte, Henrique B. Frota
& Mauri Cruz. (2)**

Vínculos de Trabalho Remunerado
nas Organizações da Sociedade Civil.
Parte 1 - Relações de Emprego (CLT),
**Helena Duarte, Henrique B. Frota
& Mauri Cruz. (3)**

Vínculos de Trabalho Remunerado
nas Organizações da Sociedade Civil.
Parte 2 - Outras Relações de Trabalho,
**Helena Duarte, Henrique B. Frota
& Mauri Cruz. (4)**

Remuneração de dirigentes das OSC
**Helena Duarte, Henrique B. Frota
& Mauri Cruz. (5)**

Dicas Jurídicas Para as
Organizações Da Sociedade Civil
Lei Geral de Proteção de Dados
Lei Federal 13.709/2018
**Helena Duarte, Henrique B. Frota
& Mauri Cruz. (6)**



Equipe **Abong**

Coordenação Institucional

Franklin Félix

Gestão Administrativo-Financeira

Adriana Torreão

Wanderson Borges

Comunicação

Danilo Feno

Patrícia França

Luiz Pires

Projetos

Pedro Bocca

Raquel Catalani

Karin Kuniyoshi

Articulação

Jhonatan Souto

Jurídico

Helena Duarte

Diretoria **Executiva**

Gestão 2019/2022

Athayde José da Motta Filho

IBASE – Instituto Brasileiro de Análises
Sociais e Econômicas (RJ)

Débora Rodrigues da Silva

Associação Vida Brasil (BA)

Eleutéria Amora da Silva

CAMTRA - Casa da Mulher Trabalhadora (RJ)

Elisety Veiga Maia

Sociedade Paraense
De Direitos Humanos (PA)

Evanildo Barbosa da Silva

FASE Nacional (RJ)

Iara Pietricovsky de Oliveira

INESC - Instituto de Estudos
Socioeconômicos (DF)

Mauri Cruz

IDhES - Instituto de Direitos Humanos,
Econômicos e Sociais (RS)




Abong

Instituto **Pólis**

Brot
für die Welt

 **FORD**
FOUNDATION

US IDEIAS
Usinas, Melhores e Projetos



Representantes **Estaduais**

ACRE

Maria Jocicleide Lima de Aguiar | RAMH

– Rede Acreana de Mulheres e Homens

BAHIA E SERGIPE

Camila Veiga de Oliveira | ELO

– Ligação e Organização (BA)

Érika Francisca de Souza | ODARA

– Instituto da Mulher Negra (BA)

Alex Federle do Nascimento | CDJBC

– Centro de Assessoria e Serviço
aos/às Trabalhadores/as da Terra
Dom José Brandão de Castro (SE)

CEARÁ

Rogério da Costa da Silva | CDVHS

– Centro de Defesa da Vida Herbert de Souza

Cristiane Faustino da Silva

| Instituto Terramar

PARÁ

Aldalice Moura da Cruz Otterloo | UNIPOP

– Instituto Universidade Popular

Maria Lindalva Melo dos Santos | MMCC

– Movimento de Mulheres do Campo
e da Cidade do Estado

PARANÁ

Cristiane Katzer | ASSESOAR

– Associação de Estudos,
Orientação e Assistência Rural

PERNAMBUCO

Alexsandra Maria da Silva | SERTA

– Serviço de Tecnologia Alternativa

Carlos Magno de Medeiros Morais

| Centro de Desenvolvimento
Agroecológico Sabiá

Sandro Cipriano Pereira | SERTA

– Serviço de Tecnologia Alternativa
(in memorian)

RIO DE JANEIRO

Carla de Carvalho Almeida da Silva | CDDH

– Centro de Defesa dos Direitos Humanos
de Petrópolis – Grupo Ação, Justiça e Paz

Diestéfano Sant’anna de Lima

| Casa de Cultura Baixada Fluminense

RIO GRANDE DO SUL

Cibele Kuss | FLD

– Fundação Luterana de Diaconia

Daniela Oliveira Tolfo | CAMP

– Centro de Assessoria Multiprofissional

Jorge Alfredo Gimenez Peralta | CEAP

– Centro de Educação e
Assessoramento Popular

SÃO PAULO

Alexandre Isaac | CENPEC

– Centro de Pesquisas em Educação
e Cultura e Ação Comunitária

Juliane Cintra De Oliveira | Ação Educativa

Luanda Mayra Chaves Teixeira | CEERT

– Centro de Estudos das Relações
do Trabalho e Desigualdades

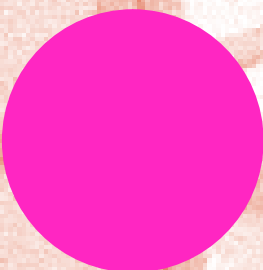
TOCANTINS

Maria Vanir Ilídio | CDHP

– Centro de Direitos Humanos de Palmas


Carleiz Pereira de Souza | COMSAÚDE

– Comunidade de Saúde Desenvolvimento
e Educação



ISBN: 978-65-00-37136-9



cadernos 
Abong



@associação.abong
@abong_osc
www.abong.org.br