LEI GERAL DE PROTEÇÃO DE DADOS
GUIA DE CONFORMIDADE MÍNIMA PARA SINDICATOS

Sistema Fiep

FIEP

Índice

Introdução

Por que a LGPD existe? Em um mercado global, onde cada vez mais a informação é o ativo mais precioso para as empresas, uma tendência desenfreada de coleta de dados foi instaurada. Com isso, diversas economias internacionais iniciaram uma regulamentação no trato de dados pessoais. A Lei Geral de Proteção de Dados é uma resposta do Brasil para o mundo, demonstrando o comprometimento das empresas que operam no Brasil com a privacidade de seus clientes, colaboradores e parceiros de negócio.

Conheça alguns conceitos que são importantes para facilitar o entendimento da legislação e favorecer a aplicabilidade de processos no seu sindicato:

Dados pessoais: toda informação relacionada à pessoa identificada ou identificável, como RG, CPF, nome, estado civil, dados de localização (GPS), entre outros.

Dados pessoais sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, que demandam um grau mais elevado de cuidado.

Penalidades: Advertência; Multa de até 2% do faturamento da pessoa jurídica ou grupo econômico, limitada a R$ 50 milhões por infração; Publicação da infração (danos reputacionais); Bloqueio/eliminação dos dados referentes à infração.

Titular dos dados: pessoa natural a quem pertence os dados.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete decisões referentes ao tratamento de dados pessoais.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza tratamento de dados pessoais em nome do controlador.

ANPD: Autoridade Nacional de Proteção de Dados, entidade governamental responsável pelo tema.

Direitos dos titulares:

- Confirmação do tratamento, acesso e correção dos dados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou em desconformidade com a lei;
- Portabilidade a outro fornecedor;
- Informação das entidades públicas e privadas com as quais o controlador compartilhou os dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento ao tratamento.

Hipóteses de tratamento:

1 Cumprimento de Obrigação legal

2 Execução de políticas públicas

3 Estudo por Órgão de Pesquisa

4 Execução de contrato

5 Exercício Regular de Direitos

6 Proteção da Vida

7 Tutela de Saúde

8 Legítimo Interesse

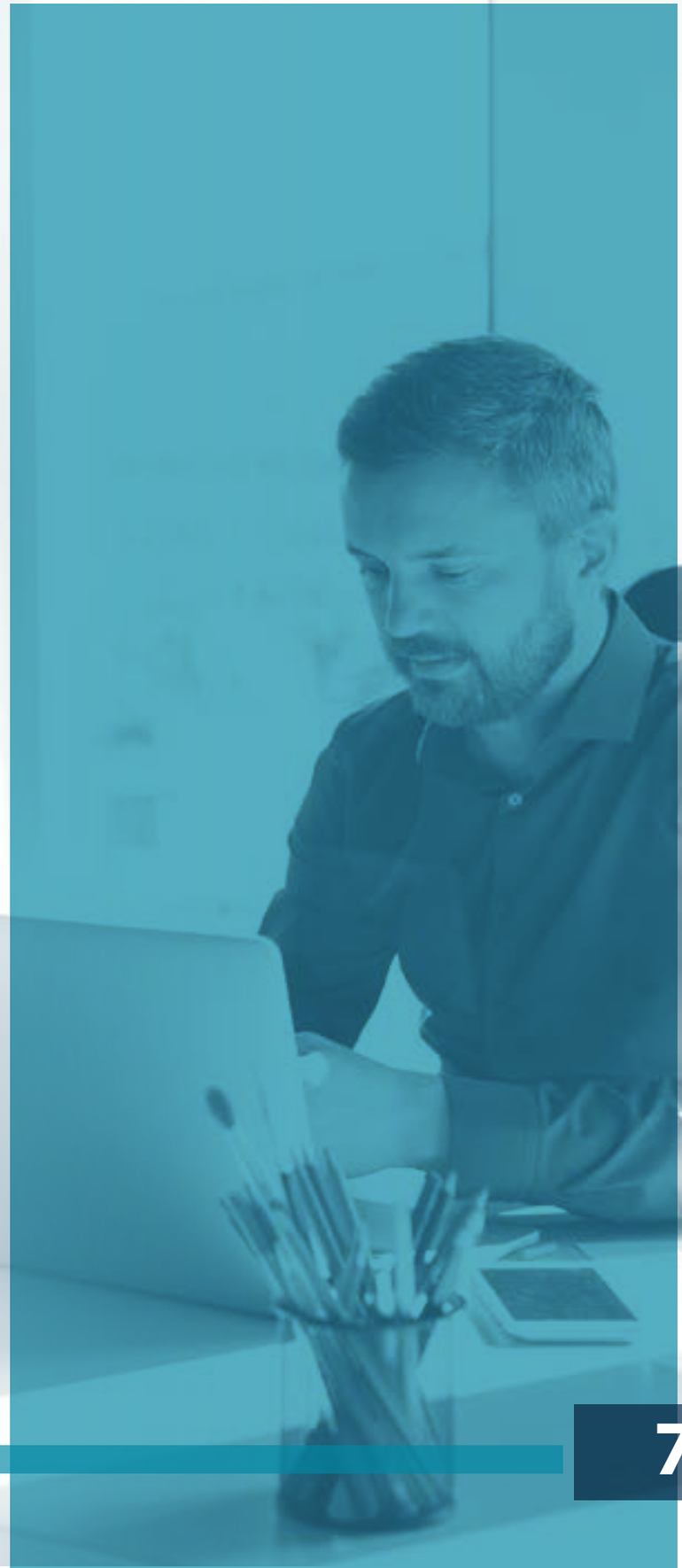
9 Proteção ao Crédito

10 Consentimento

O Sistema Fiep tem a missão de trazer para você, sindicato associado, não apenas os conceitos básicos presentes na lei, mas sim, uma abordagem prática do que devemos realizar para estar em conformidade com a lei.

A seguir, apresentamos um modelo básico para esta conformidade mínima. Leia com atenção e esperamos que seja de grande utilidade.

PROJETO DE CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS



1. Autoanálise

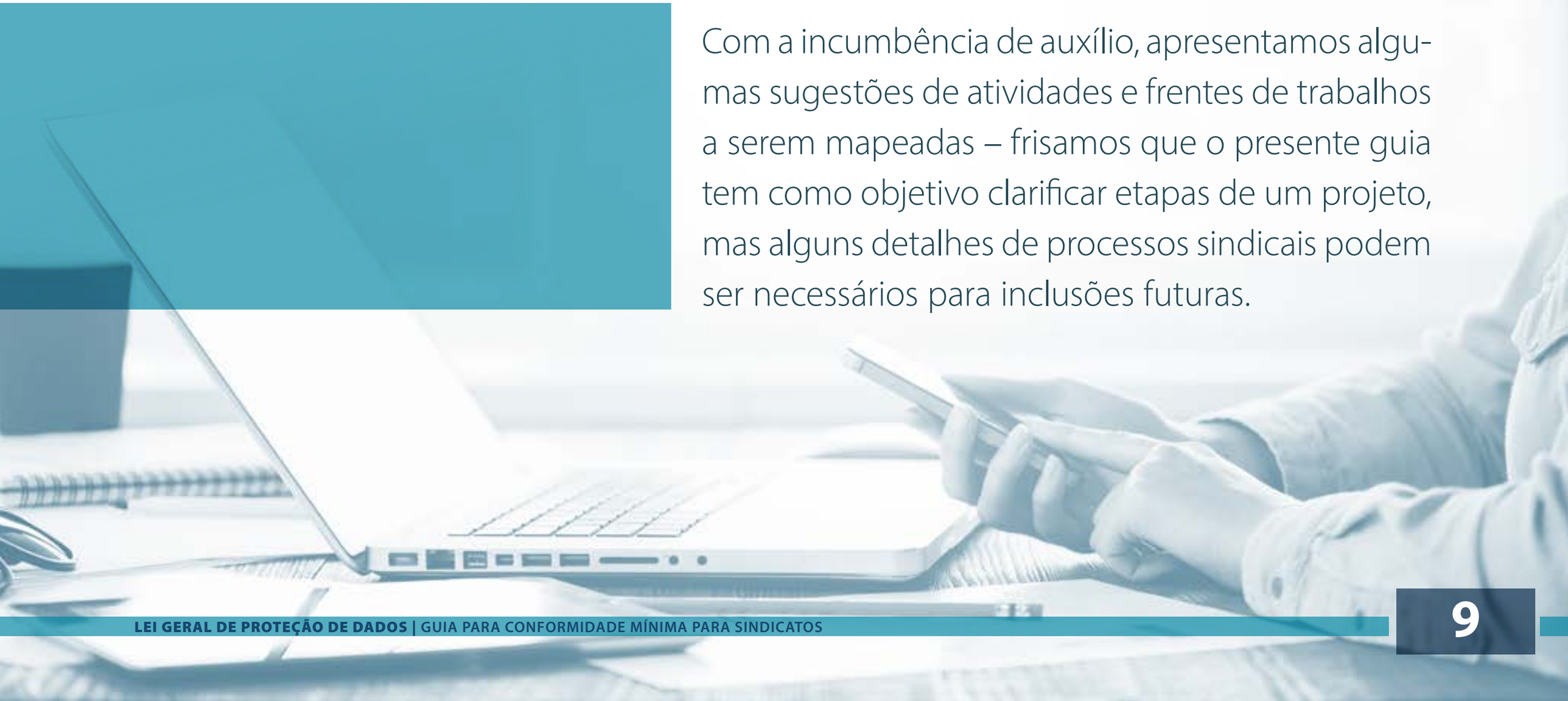
A primeira análise desta cartilha é uma dúvida para diversos sindicatos: "essa lei se aplica para nós?". O 3º artigo da lei define que "*Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio.*" Essa dúvida é bastante comum, afinal, ao iniciar uma leitura da lei, parece que o direcionamento é enquadrado para grandes corporações, algo muito distante da nossa realidade – sindicatos de menor porte que, na maioria das vezes, possuem uma estrutura de pessoal extremamente

enxuta, com apenas um colaborador. Mas, como pudemos evidenciar, a Lei Geral de Proteção de Dados não define sua aplicabilidade por tipo de operação ou porte da empresa.

Independente do porte do sindicato, devemos entender que a lei permeia todas as áreas da organização. E a melhor forma de iniciarmos este engajamento é obtendo o apoio da alta administração. A cultura do exemplo é viva nas organizações, sendo assim, apresente a lei aos seus diretores, esse é o primeiro público a ser conscientizado. Com algumas leituras sobre a lei (sim, uma única leitura não trará clareza o suficiente) a decisão é: esse trabalho será conduzido pelo time interno ou devemos

contratar uma consultoria especializada? Não existe resposta certa ou errada para esta pergunta. Um trabalho conduzido por colaboradores é profundo e menos custoso. Uma consultoria especializada pode ser mais ágil e assertiva nos planos de ação. Caso opte pela condução interna, um aviso: esse trabalho exige dedicação.

Com a incumbência de auxílio, apresentamos algumas sugestões de atividades e frentes de trabalhos a serem mapeadas – frisamos que o presente guia tem como objetivo clarificar etapas de um projeto, mas alguns detalhes de processos sindicais podem ser necessários para inclusões futuras.



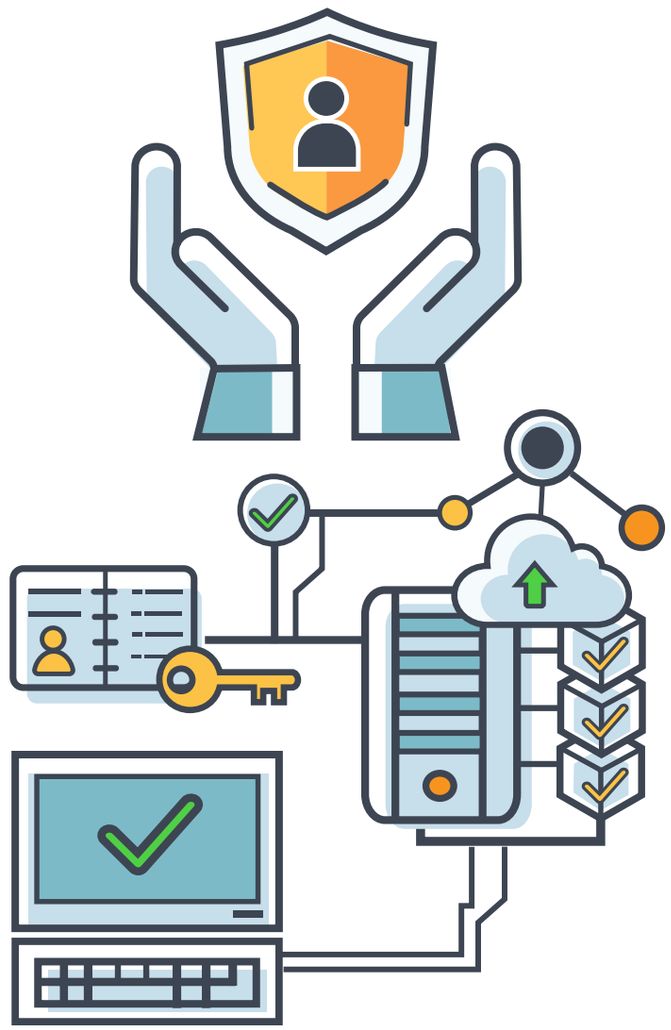
2. DPO – Encarregado de Dados

ARTIGO 9 ➡ CANAL DE ATENDIMENTO DO DPO
ARTIGO 18 ➡ COMPLEMENTAR AO 9
ARTIGO 19 ➡ COMPLEMENTAR AO 9
ARTIGO 11 ➡ HIPÓTESES PARA TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
ARTIGO 41 ➡ NOMEAÇÃO DPO
ARTIGO 48 ➡ COMUNICAÇÃO DE INCIDENTE COM DADOS
ARTIGO 50 ➡ GOVERNANÇA DE DADOS

A *General Data Protection Regulation*, legislação europeia que inspirou a LGPD, tem na figura do DPO (*Data Protection Officer*) o responsável pelas diretrizes de tratamento de dados nas organizações. A LGPD tem a mesma figura, nomeada como Encarregado de Dados. Após a primeira etapa, autoanálise, compete ao sindicato avaliar onde o Encarregado de Dados melhor se encaixa, podendo ser um colaborador ou um terceiro especializado.

Para melhor direcionar sua análise de quem deve assumir esta (grande) tarefa, pontuamos algumas responsabilidades do Encarregado:

a. Educar diretores e os funcionários do sindicato sobre requisitos de privacidade de dados pessoais importantes.



b. Treinamento e posicionamentos para pessoal envolvido no processamento de dados.

c. Interagir com a Autoridade Nacional de Proteção de Dados.

d. Manter registros abrangentes de todas as atividades de processamento de dados realizadas pelo sindicato, incluindo o objetivo de todas as atividades de processamento, que devem ser tornadas públicas mediante solicitação.

e. Atender os titulares de dados em nome do sindicato, tirando dúvidas sobre como seus dados estão sendo usados, seus direitos de exclusão de dados pessoais e quais medidas o sindicato adotou para proteger suas informações pessoais.

Este "porta-bandeira" da privacidade terá um papel chave durante o seu projeto de conformidade à LGPD, mas também terá obrigações recorrentes com a lei. Como explicado no item "e", a interface com os titulares de dados será constante. A Lei Geral de Proteção de Dados indica que todas as organizações deverão dispor de um canal de atendimento para demandas de privacidade junto aos seus clientes. Este canal pode ser um sistema dedicado, pode ser um formulário ou até um e-mail, mas ele deve existir. Recomendamos que revise a parte de "Direito dos Titulares", explicada anteriormente em nosso guia, para que visualizem quais as possíveis demandas que serão atendidas pelo DPO. Esse canal deve estar disponibilizado ao titular dos dados no site do sindicato, incluindo o endereço de contato para tratativas e a nomeação do Encarregado de Dados do sindicato.

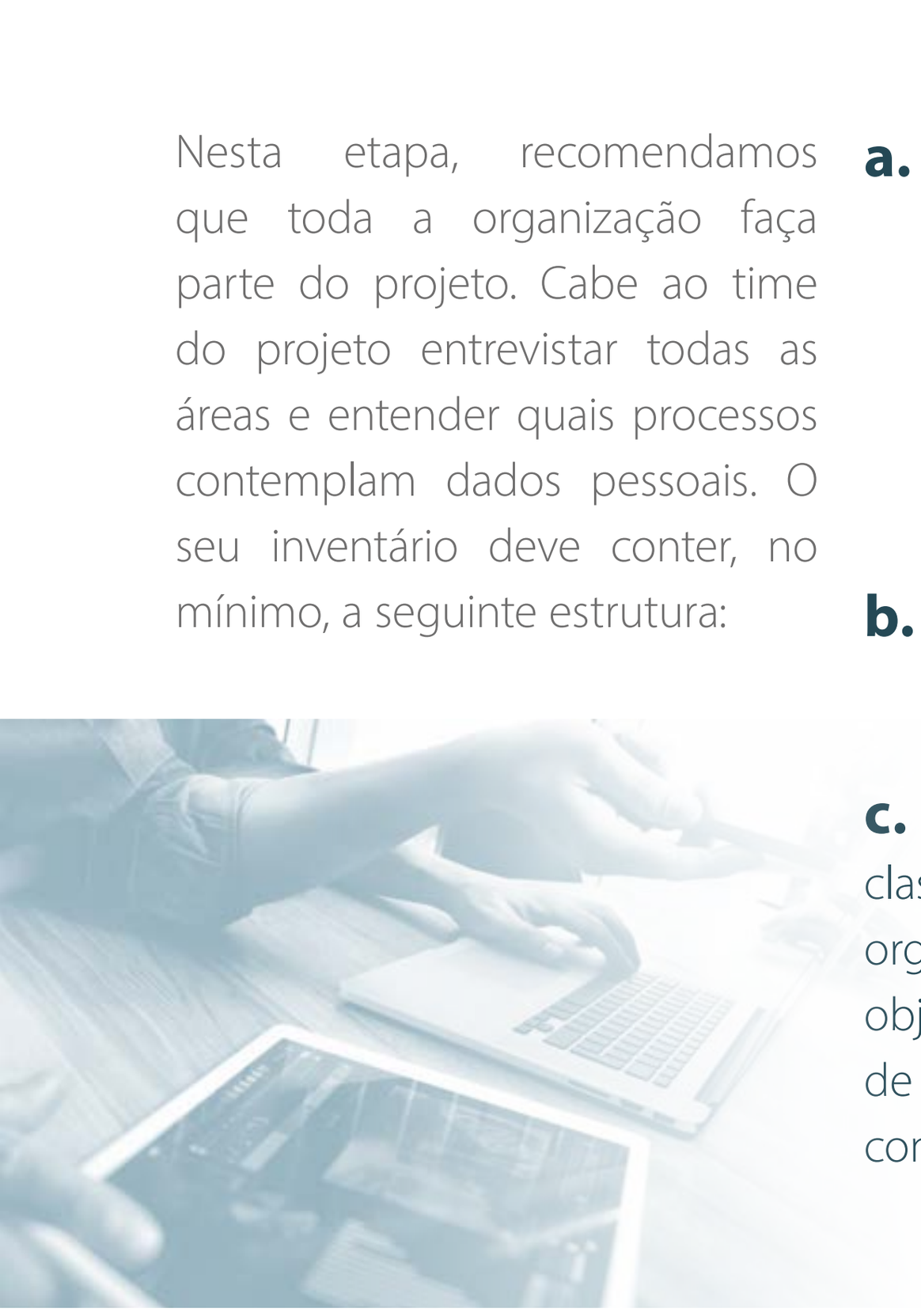
Outro aspecto fundamental do Encarregado de Dados é o relacionamento com os parceiros de negócio do sindicato. Um exemplo frequente são eventos e workshops, usualmente realizados em parceria com outras empresas. As inscrições destes eventos coletam diversos dados pessoais, que eram utilizados com diversas finalidades e compartilhamentos. Essa prática deve ser avaliada e, se necessário, proibida pelo DPO. O compartilhamento de dados deve ser autorizado pelo titular dos dados, ou seja, toda vez que essa prática se fizer necessária, deve ser informada previamente ao titular. Além disso, todos os tratamentos de dados pessoais devem ser zelados pelo Encarregado de Dados, representando o sindicato nessas questões e zelando sempre pelo cumprimento da Lei Geral de Proteção de Dados.

3. Gestão de Dados

ARTIGO 6 ➡ PRINCÍPIOS DOS TRATAMENTOS DE DADOS
ARTIGO 7 ➡ HIPÓTESES DE TRATAMENTO DE DADOS
ARTIGO 37 ➡ INVENTÁRIO DE DADOS

A lei fala em proteção de dados pessoais, mas como iremos proteger tais dados se não os identificamos? Sem dúvidas, a maior etapa do projeto em tempo de execução é o Inventário de Dados. E não, não tem como fugir. O artigo 37 deixa claro que toda empresa, no caráter de controlador ou operador, deve manter registro das suas operações de tratamento de dados. Pense o seguinte: caso indagado por um titular de dados (na figura de um associado), por um parceiro de negócio ou pela própria Autoridade Nacional de Proteção de Dados (a agência governamental responsável pelo tema, também conhecida por ANPD), a empresa deve responder quais os dados pessoais são tratados em seus processos.

Nesta etapa, recomendamos que toda a organização faça parte do projeto. Cabe ao time do projeto entrevistar todas as áreas e entender quais processos contemplam dados pessoais. O seu inventário deve conter, no mínimo, a seguinte estrutura:



a. Mapeamento indicando o processo, quais dados são coletados, quem é o titular destes dados, para qual finalidade os dados são coletados, onde estes dados são armazenados, quem tem acesso, por que estes dados são coletados e qualquer outra informação que sua organização acredite ser relevante para maior compreensão deste mapeamento.

b. Após o mapeamento dos dados, avaliar qual das 10 hipóteses descritas na LGPD para tratamento embasa a coleta.

c. Aconselhamos que os sindicatos apliquem uma classificação do risco do tratamento para otimizar sua organização – dividida como "baixo, médio e alto". O objetivo desta classificação é criarmos uma priorização de quais processos apresentam maior risco de conformidade e, portanto, devem ser tratados primeiro.

Esse mapeamento deve existir. Como ele irá ser feito, depende de cada organização. Existem prestadores de serviço que ofertam soluções tecnológicas para tal, inclusive o Senai, mas qualquer forma de registro organizado é recomendada, principalmente o "bom e velho" Excel. Adicionalmente, a ANPD divulgou em seu site modelos de planilhas para preenchimento e execução do inventário de dados. Os arquivos são extremamente organizados e práticos, além de gratuitos – https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd .

Lembre-se, este documento é vivo. Constantemente, novos tratamentos irão começar na organização, e sempre devem ser registrados no inventário.

4. Gestão de Processos

Esta etapa é uma consequência natural do inventário de dados. Depois de entender todos os processos e tratamento de dados existentes na organização, após priorizar os riscos de conformidade à LGPD em cada um destes, como podemos tratá-los? Existem, dentre outras opções, duas formas claras: tecnologia (item 6 do nosso guia) e processos.

O processo pode ser revisitado para diminuição destes riscos, buscando soluções práticas, como estas:

a. Identificação se algum dos dados pessoais coletados excede a finalidade do processo, podendo ser retirado da coleta e excluído da base de dados.

b. Validação para troca de ferramentas de envio de dados pessoais que não apresentam a segurança desejada.

c. Digitalização de documentos físicos com dados pessoais, arquivando em ambientes tecnológicos seguros.

d. Centralização de processos com dados pessoais sensíveis – remover do fluxo de informações pessoas que não participem diretamente do processo. Exemplo: colaboradores em excesso copiados no e-mail.

5. Minutas Contratuais

ARTIGO 7 – INCISO V ➡ O ARTIGO MOSTRA AS DEZ HIPÓTESES DE TRATAMENTO DE DADOS, E O ITEM VINCULA A CONTRATOS.
ARTIGO 8 ➡ O ARTIGO TRATA DE CONSENTIMENTO
ARTIGO 14 ➡ TRATAMENTO DE MENORES DE IDADE
ARTIGO 39 ➡ DETERMINAÇÃO CONTROLADOR X OPERADOR

Como comentamos anteriormente, a LGPD dispõe de 10 hipóteses legais para tratamento de dados pelas empresas, e uma delas é a execução de contrato – em outras palavras, todo contrato celebrado entre as partes titulares que registre o tratamento de dados pessoais e os discrimine, resguarda a empresa durante a vigência do mesmo. Sendo assim, constatamos que os contratos firmados são de suma importância para segurança jurídica da organização no que tange a LGPD. Mas temos outros pontos importantes a destacar, são eles:

a. Revisite todas as minutas contratuais do sindicato – inclua cláusulas de privacidade de dados, discriminando quais dados pessoais são coletados durante o processo, para qual finalidade são utilizados e por quanto tempo serão armazenados. Como auxílio, inserimos ao fim do nosso documento um modelo de aditivo contratual para atendimento da LGPD – Anexo A.

b. Cabe ao operador de dados realizar o tratamento mediante as instruções do controlador. Por isso, caso a sua organização colete dados pessoais e compartilhe com parceiros de negócio, recomendamos que todas as instruções cabíveis sejam formalizadas em aditivos contratuais, definindo responsabilidades e criando transparência para a relação de tratamento de dados entre as

partes. Lembre-se, seu parceiro de negócio é corresponsável pelo tratamento de dados perante a ANPD (Autoridade Nacional de Proteção de Dados).

c. Coleta de dados que não são firmadas em contratos, e não possuem outra hipótese legal para tratamento, devem ser suportadas por um Termo de Consentimento. Este documento nada mais é do que uma autorização do titular dos dados para que esse tratamento possa ocorrer – vale salientar que o mesmo é revogável. O Termo de Consentimento deve firmar quais os dados são coletados, para qual finalidade, por quanto tempo serão armazenados e deve dispor de um canal de comunicação junto ao DPO da organização. Como auxílio, inserimos ao fim do nosso documento um modelo de termo

de consentimento com estrutura padronizada para atendimento da LGPD – Anexo B. Lembre-se, esse modelo contém informações básicas, quanto mais o termo transparecer ao titular o tratamento de dados realizado, mais seguro este documento é.

d. Caso o público-alvo do Termo de Consentimento seja composto de menores de idade, vale salientar que o consentimento deve ser específico e só pode ser realizado por um dos pais ou responsável legal do menor.

6. Tecnologia

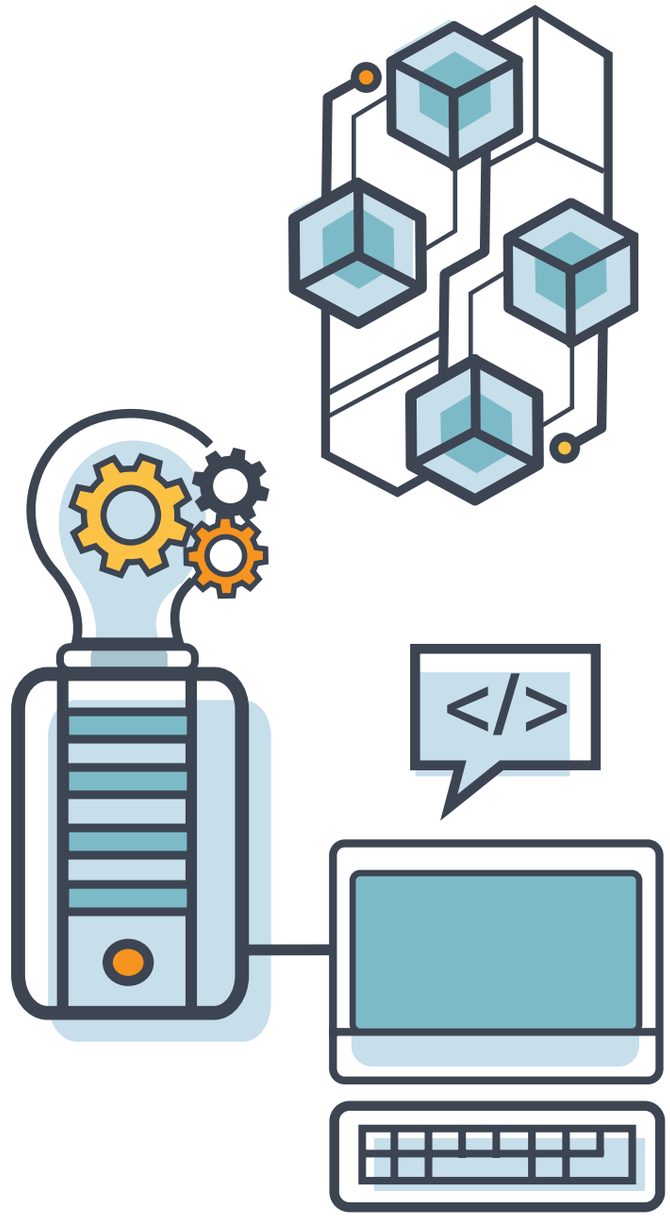
ARTIGO 6 – INCISO 7 ➡ O ART. 6º FALA SOBRE AS BOAS PRÁTICAS PARA O TRATAMENTO DE DADOS. NO ITEM 7, DE MANEIRA DIRETA, FALA-SE SOBRE A NECESSIDADE DE SEGURANÇA DE DADOS.
ARTIGO 12 ➡ ARTIGO DEDICADO À ANONIMIZAÇÃO DE DADOS
ARTIGO 46 ➡ ARTIGO DEDICADO À PROTEÇÃO DE DADOS PESSOAIS
ARTIGO 47 ➡ ARTIGO DEDICADO À SEGURANÇA DA INFORMAÇÃO, MESMO APÓS O TRATAMENTO DE DADOS
ARTIGO 49 ➡ ARTIGO DEDICADO A DEFINIR QUE SISTEMAS DEVEM SER ESTRUTURADOS NAS BOAS PRÁTICAS DE GOVERNANÇA, ACESSO E SEGURANÇA.

É importante frisarmos o seguinte: independentemente do tipo de organização, hoje as maiores concentrações de dados são encontradas no ambiente tecnológico. Claro, qualquer tipo de relatório ou base sistêmica pode ser impresso, qualquer coleta de dados pode ocorrer via formulário físico, mas a realidade é que, tendo em vista que a lei tem como premissa a proteção de dados pessoais, o maior risco de vazamento está na esfera tecnológica. Sendo assim, a LGPD é direta: as empresas devem investir e comprovar recursos e comprometimento com a segurança de dados pessoais – de clientes, colaboradores ou parceiros de negócio. Mas como evidenciar essas atividades? Como transformar os artigos referenciados acima em ações? Vamos lá:

a. Todas as medidas de segurança tecnológica que permeiam um programa, seguindo boas práticas de mercado, correspondem ao que chamamos de SEGURANÇA DA INFORMAÇÃO. Referências de controles para um programa de segurança da informação satisfatório estão descritos na norma ISO/IEC 27701.

b. Definições de documentos normativos que orientem o sindicato e seus parceiros de negócio são essenciais – Política de Segurança da Informação, Política de Privacidade de Dados e Processos de Respostas a Incidentes.

c. Anonimização de dados – tornar um dado pessoal anonimizado é processá-lo de forma que ele não seja identificável. Assim, em caso de vazamentos, os titulares dos dados não sofrem prejuízo algum. Existem ferramentas de mercado que auxiliam na anonimização de bases, altamente recomendável para empresas com um alto volume de dados pessoais sensíveis.



d. Com a LGPD, seu processo de contratação deve ser revisto. Fornecedores de sistemas e aplicativos devem comprovar certificações e capacidades técnicas de ofertar o produto contratado com segurança, tendo em vista que dados de colaboradores, clientes e parceiros de negócio serão armazenados.

e. Gestão de acessos – quanto menos pessoas tiverem acesso a bases de dados pessoais, menor a chance de vazamento. Sendo assim, invista em um processo que estrutura uma gestão de acesso confiável na organização, com autorização para concessão de acessos e revisões periódicas. Apenas colaboradores ou terceiros que tenham necessidade operacional devem acessar bases de dados pessoais.

f. Controles tecnológicos – implementação de ferramentas tecnológicas, como *firewalls*, análises de vulnerabilidade e antivírus.

Adicionalmente, algumas "mudanças práticas" devem ser implementadas de imediato – para conformidade imediata com a lei. O site do Sindicato deve refletir algumas mudanças básicas do projeto de conformidade à LGPD. São elas: a) Inclusão de um aviso sobre coleta de dados como IP de navegação e *cookies* – os dados de navegação são considerados dados pessoais, sendo assim, devemos deixar claro ao usuário sua coleta e tratamento; b) Inclusão da Política de Privacidade do sindicato, para conhecimento de associados e parceiros de negócio sobre as diretrizes de tratamento de dados da organização.

7. Gestão da Mudança

ARTIGO 41 – ITEM 3 ➡ O ITEM DESCREVE A IMPORTÂNCIA DE O ENCARREGADO DE DADOS ORIENTAR COLABORADORES SOBRE PRÁTICAS DE PRIVACIDADE.

O presente tópico é essencial para qualquer projeto de sucesso. Observamos que a conformidade com a LGPD demanda alteração nos contratos elaborados pelas empresas, no modo que as empresas interagem com clientes e no ambiente tecnológico das organizações. Mas qual o denominador comum em todos esses processos? Sim, pessoas. Não importa o quanto as empresas invistam recursos físicos e operacionais para proteção de dados, se os seus colaboradores não tiverem o engajamento com esta prática, o ambiente apresenta um risco considerável de vazamento.

O engajamento dos colaboradores tem algumas premissas. Antes de apontá-las, é importante dizer que este processo requer esforço e tempo, pois nenhuma cultura é transformada de uma hora para outra. Aqui, listamos algumas ações para conscientização geral na organização:

a. O engajamento da diretoria do sindicato é essencial para que seus colaboradores sigam o exemplo. Como mencionamos no 1º item (Autoanálise), o compromisso dos diretores com o tema é crucial para o sucesso do projeto de conformidade com a lei. Sendo assim, aconselhamos que apresentem e conversem sobre a relevância da lei em reuniões com o público, demonstrando os impactos sobre sua indústria e as relações sindicais – lembrem-se de registrar essas reuniões em ata, gerando uma evidência do comprometimento do sindicato com a disseminação do conhecimento da LGPD.

b. Comunicados de conscientização periódicos, para que todos se familiarizem com os termos da LGPD e suas práticas. Utilize

o canal de comunicação que atinja a maioria dos colaboradores – e-mail, cartazes, folhas impressas em elevadores etc.

c. Treinamento dedicado à Lei Geral de Proteção de Dados, com certificado ou outra evidência de realização por colaborador – uma forma de evidenciar o comprometimento da companhia para conscientização de todos.

d. Inclusão de tópico dedicado à privacidade no Código de Conduta do sindicato. É importante frisar que o comprometimento com a privacidade é uma conduta desejada para o corpo de colaboradores.

e. Aos poucos, deixe de referenciar a LGPD como norteador comportamental e adote termos como "Cultura de Privacidade" ou "Cultura Organizacional". A conformidade com a lei tem que deixar de ser uma obrigação e passar a ser comportamental, pensando na perpetuidade do assunto.

Por fim, e não menos importante, todos os sindicatos possuem parceiros de negócio. Alguns destes, essenciais para a operação de suas atividades. Como a Lei Geral de Proteção de Dados trata da corresponsabilidade entre Controlador e Operador (definições realizadas no início do documento), a conscientização dos parceiros de negócio torna-se tão importante quanto a de colaboradores. Identifique quais são os mais importantes e realize reuniões de discussão sobre o tema, buscando o engajamento de todos.

Ficou com alguma dúvida? Você pode se inspirar nos materiais de Privacidade do próprio Sistema Fiep:

Página de Proteção e Privacidade de Dados do Sistema Fiep:

https://www.sistemafiep.org.br/protecao-e-privacidade-de-dados-1-33676-454470.shtml

Política de Privacidade de Dados do Sistema Fiep:

https://www.sistemafiep.org.br/uploadAddress/Politica-de-Privacidade-de-Dados[96993].pdf

Canal de Atendimento:

https://www.sistemafiep.org.br/privacidade-de-dados-pessoais/

ANEXO A

Contrato n. xxxx

PRIMEIRO TERMO ADITIVO AO CONTRATO N. XXXXXXX CELEBRADO EM XX/XX/XXXX ENTRE O SINDICATO XXXXX E O PARCEIRO XXXXXX

Pelo presente instrumento, de um lado, o sindicato XXXXXXX, (doravante "SINDICATO") e, de outro lado, o parceiro XXXXXXX, (doravante "PARCEIRO"), ambos devidamente qualificados no contrato em epígrafe, por seus legais representantes ao final assinados, e CONSIDERANDO que, em XX/XX/XXXX, as partes firmaram Contrato de XXXX, tendo como objeto XXXXX; e, CONSIDERANDO que, para fins de conformidade legal à Lei Geral de Proteção de Dados Pessoais (LGPD - Lei n. 13.709/2018), as Partes têm interesse em alterar e/ou incluir as seguintes previsões no contrato; *ISTO POSTO*, as Partes têm entre si certo e ajustado o Primeiro Termo Aditivo ao Contrato XXXXXX, que será regido pelas cláusulas e condições a seguir dispostas, pelas quais se obrigam por si, seus herdeiros e seus sucessores na melhor forma de direito, decidindo, portanto, alterar e/ou incluir as seguintes previsões no Contrato:

CLÁUSULA XXXXXX - DA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS

1. O PARCEIRO se obriga a:

a) Cumprir as normas de proteção de dados aplicáveis à espécie, notadamente a Lei Federal 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - "LGPD");

b) Observar as políticas de privacidade e de tratamento de dados do SINDICATO, especialmente no que tange a relações com terceiros;

c) Possuir estrutura operante para recepcionar e atender, de forma adequada, petições e/ou comunicações dos titulares de dados pessoais, nas quais seja exigido o cumprimento a qualquer dos direitos previstos na LGPD;

d) Guardar registro de todas as operações de tratamento de dados efetuadas durante a relação jurídica entre as PARTES, de forma estruturada, sempre que for necessário para cumprir a LGPD;

e) Adotar as medidas técnicas e organizacionais adequadas para garantir a segurança e a confidencialidade dos dados pessoais tratados, de acordo com as melhores práticas de tecnologia e segurança da informação;

f) Possuir Plano de Prevenção e Resposta a Incidentes com vazamento de dados, bem como Comitê de Gestão de Crises, ambos ativos e operantes;

g) Caso ocorra um incidente envolvendo dados pessoais, notificar a outra PARTE no prazo máximo de 3 (três) dias úteis após a gerência ter ciência do mesmo, descrevendo, se possível, a natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; os riscos relacionados ao incidente; os motivos da demora, no caso de a comunicação não ter sido imediata; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;

h) Obter a anuência prévia do SINDICATO, por escrito, para fins de qualquer subcontratação ou compartilhamento para terceiro de dados pessoais durante a relação jurídica entre as PARTES, bem como garantir a submissão desse terceiro às mesmas obrigações do PARCEIRO no que se refere à confidencialidade e ao atendimento à legislação de proteção de dados pessoais;

i) Imediatamente ao final da vigência do presente Contrato, excluir todo e qualquer dado pessoal acessado através do SINDICATO, com exceção dos dados que devem ser mantidos por obrigação legal ou outra base legal estabelecida em lei, estando apta a comprovar ao SINDICATO essa exclusão de dados, sempre que for solicitada.

2. Para todos os efeitos legais, o PARCEIRO expressamente declara que:

a) Efetuou o mapeamento de todas as suas operações de tratamento de dados, e que nenhum dado pessoal é tratado sem o devido enquadramento em pelo menos uma das hipóteses legais previstas nos artigos 7º e 11 º, da LGPD, e do respeito aos princípios norteadores do artigo 6º, da LGPD;

b) Nomeou um Encarregado (DPO), o qual está apto a atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Parágrafo Único: O PARCEIRO isentará o SINDICATO de qualquer demanda administrativa, judicial ou extrajudicial relacionada ao descumprimento das obrigações por culpa exclusiva do PARCEIRO no que se refere ao tratamento de dados pessoais, cabendo exclusivamente ao PARCEIRO ressarcir quaisquer quantias que, eventualmente, o SINDICATO seja obrigado a desembolsar em decorrência de condenações judiciais, sanções administrativas, multas, compensações, juros, danos e prejuízos em geral, relacionados à proteção de dados pessoais, que decorram de culpa exclusiva do PARCEIRO, no prazo máximo de 60 (sessenta) dias após ter sido interpelada extrajudicialmente pelo SINDICATO.

Ratificam as Partes todas as demais cláusulas e disposições do Contrato, bem como dos Anexos, que não tenham sido expressamente alteradas pelo presente instrumento e que não conflitem com o aqui estipulado, as quais permanecem integralmente em vigor.

E por estarem justas e acordadas, as Partes assinam o presente termo aditivo, em 02 (duas) vias de igual teor e forma, na presença de 02 (duas) testemunhas.

Curitiba, (data atualizada)

_____
SINDICATO XXXXXXX
Nome:
Cargo:
CPF:

_____
PARCEIRO XXXXXXX
Nome:
Cargo:
CPF:

ANEXO B

Termo de Consentimento de dados | Sindicato XXXXX

O presente documento evidencia quais os dados são coletados e qual a finalidade do seu uso.

1. Informações coletadas

Coletamos dados pessoais para cadastro dos participantes, tais como: nome completo, e-mail, telefone, nome da empresa, cargo, cidade e estado.

2. Uso das informações coletadas

Ao aceitar este termo, você nos concede autorização para que as informações que coletamos sejam armazenadas em nossos bancos de dados por 02 (dois) anos, e que possam ser usadas com o objetivo de:

a) Promover capacitação técnica que o Sindicato XXXXX se propõe;
b) Recebimento de comunicação de cursos e ofertas do Sindicato XXXXX;
c) Compartilhar os dados junto ao XXXXXXXX, organização parceira do evento;
d) Armazenar e utilizar os dados coletados para fins de atendimento a obrigações legais ou regulatórias requisitadas ao Sistema Fiep em concordância rigorosa com a Lei Geral de Proteção de Dados (lei nº 13.709/2018).

3. Política

Fica acordado que você não promoverá ações em desacordo com as diretrizes e recomendações da nossa Política de Privacidade, disponível no link: XXXXXXXX .

4. Atualização, correção ou exclusão de informações

Você poderá solicitar junto ao DPO (Encarregado de Dados) do Sindicato XXXX a exclusão das informações de nossos bancos de dados. É importante que você saiba, porém, que essa exclusão não será automática, ou seja, você precisa solicitar formalmente esta exclusão através do endereço eletrônico do responsável: ENDEREÇO DE EMAIL OU LINK DA FERRAMENTA DE ATENDIMENTO DO DPO.

5. Disposições gerais

Para a sua segurança, a capacitação está condicionada à aceitação destes termos de uso. Isso quer dizer que você está concordando com todos os termos desta política e se responsabiliza por ficar atento às suas alterações. Por isso, leia com cuidado estes termos, ok?

Sistema Fiep

FIEP