

GUIA ORIENTATIVO AOS SINDICATOS

LGPD - LEI GERAL DE PROTEÇÃO DE DADOS

BLOCOS 1e2
O GUIA TERÁ 5 BLOCOS

São Paulo, maio de 2021.



PALAVRA DO PRESIDENTE

A Federação das Indústrias do Estado de São Paulo (Fiesp), apresenta o Guia LGPD aos Sindicatos, um complemento à Cartilha de Proteção de Dados Pessoais. O Guia traz orientações objetivas e informações sobre a Lei Geral de Proteção de Dados para que nossos sindicatos, bem como toda e qualquer entidade, possam ter em mãos um instrumento de auxílio e se adequarem.

Diante de diversos desafios para a implementação da LGPD, a Fiesp tem realizado, com muito orgulho e dedicação, um imenso esforço para auxiliar nossos sindicatos e empresas nesta adequação, por meio de cartilhas, palestras, seminários, cursos, entre outras relevantes campanhas de conscientização.

Desde 2015, com a criação de grupos de trabalho dedicados e através de congressos e seminários, temos orgulho de nos debruçarmos de forma profunda sobre o tema da Segurança e Defesa Cibernética e Proteção de Dados, promovendo conhecimento para toda a sociedade. Agora, com a vigência deste importante marco normativo para o Brasil, não será diferente.

As ações não param por aqui. Ainda tem muito a ser feito e nós estaremos sempre ativos e empenhados em apoiar os sindicatos, as indústrias e a sociedade brasileira.

Grande abraço,

Paulo Skaf
Presidente

INTRODUÇÃO

Com a aprovação em 2018 da Lei Geral de Proteção de Dados – LGPD brasileira e o funcionamento da Autoridade Nacional de Proteção de Dados – ANPD, fica ainda mais clara a relevância do tema e a necessidade de atenção da sociedade para o tratamento de Dados Pessoais coletados no dia a dia.

Com a intenção de apoiar os Sindicatos na contínua gestão adequada de Dados Pessoais, a Federação das Indústrias do Estado de São Paulo – FIESP elaborou um Guia Orientativo, exemplificativo e acessível à realidade sindical.

Neste Guia apresentaremos informações sobre a LGPD e a ANPD, indicaremos os principais passos para conformidade - especialmente voltados para adequar as relações de trabalho, institucionais e administrativas - bem como responderemos as principais dúvidas provenientes dos sindicatos, que estruturamos no formato de um FAQ.

De forma objetiva e simplificada, o Guia Orientativo aos Sindicatos busca trazer esclarecimentos e direcionamentos em relação à nova Lei, para que os Sindicatos possam realizar um uso seguro e ético de Dados Pessoais, cumprindo as regras estabelecidas na LGPD.

ESTRUTURA DO GUIA AOS SINDICATOS

PROPOSTA



- Um Guia Orientativo, exemplificativo e acessível à realidade sindical;
- Consolidar alguns conceitos: Definição de Dado Pessoal; Dado Sensível, com exemplificação;
- Direcionamento para a adequação à LGPD: Baseado nas respostas do questionário enviado;
- Direitos fundamentais dos usuários (Legislação);
- Penalidades para não cumprimento da Lei.

ESTRUTURA DE ENVIO DOS MATERIAIS

1º BLOCO

1. O que o sindicato precisa saber: Legislação
2. Glossário Exemplificativo
3. Passo a passo para adequação

2º BLOCO

4.1 Relações de Trabalho

3º BLOCO

4.2 Relações Institucionais

4º BLOCO

4.3 Relações Administrativas

5º BLOCO

5. Perguntas Frequentes (FAQ)

ÍNDICE

1. LEGISLAÇÃO	7
1.1. A LEI GERAL DE PROTEÇÃO DE DADOS	7
1.2. LGPD E SINDICATOS	11
1.3. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS	12
2. GLOSSÁRIO EXEMPLIFICATIVO	16
3. PRINCIPAIS PASSOS PARA ADEQUAÇÃO	19
3.1. ENVOLVIMENTO DA EQUIPE	19
3.2. ESTABELEÇA UM LÍDER (ENCARREGADO - DPO)	19
3.3. ESTABELEÇA UM CANAL DE COMUNICAÇÃO	21
3.4. ESTABELEÇA PONTOS FOCAIS NOS DEPARTAMENTOS DOS SINDICATOS	21
3.5. REÚNA INFORMAÇÕES SOBRE OS DADOS COLETADOS - MAPEAMENTO	21
3.6. ANALISE SE OS DADOS ESTÃO SENDO TRATADOS CONFORME A LGPD - DIAGNÓSTICO	22
3.7. BUSQUE FERRAMENTAS OU UTILIZAÇÃO DE BANCO DE DADOS CENTRALIZADO	22
3.8. CONSTRUÇÃO DO PROGRAMA DE GOVERNANÇA	22
3.9. DOCUMENTOS JURÍDICOS	23
3.10. TREINAMENTO PARA CONSCIENTIZAÇÃO	23
4. COMO SE ADEQUAR.....	25
4.1. RELAÇÕES DE TRABALHO	25
4.1.1. DADOS PESSOAIS TRATADOS NOS PROCESSOS DA RELAÇÃO DE TRABALHO	26
4.1.2. TRANSMISSÃO DE DADOS PESSOAIS DECORRENTES DA RELAÇÃO DE TRABALHO A TERCEIROS	32

LEGISLAÇÃO

LEGISLAÇÃO

1.1 A LEI GERAL DE PROTEÇÃO DE DADOS

Aprovada em 14 de agosto de 2018 e baseada na legislação europeia denominada General Data Protection Regulation (GDPR), a Lei Geral de Proteção de Dados (LGPD – Lei 13.709/18) entrou em vigor em 18 de setembro de 2020, após anos de debates, com o objetivo de centralizar normas relacionadas à privacidade e proteção de Dados Pessoais, inclusive nos meios digitais, antes pulverizadas em normas setoriais, como o Código de Defesa do Consumidor. A LGPD, portanto, vem com o intuito de gerar maior segurança jurídica para as organizações, bem como proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, estabelecendo regras e limites a respeito da coleta, armazenamento, utilização, compartilhamento e demais operações de tratamento de Dados Pessoais dos indivíduos (denominados “titulares”, pela Lei).

No caso dos sindicatos e associações, diversos Dados Pessoais também são tratados diariamente e registrados para o envio, por exemplo, de comunicados, convites, informativos, cobranças de anuidade ou mensalidade, e outras atividades. Logo, Dados Pessoais como CPF, RG, e-mail e até mesmo cargo precisam de atenção no tratamento.

A Lei é importante para o Brasil em razão da harmonização e atualização de conceitos, gerando maior segurança jurídica; atração de investimentos do exterior e diferencial competitivo, diante do nível de proteção legal que agora contamos, assim como fomento cultural em proteção de Dados Pessoais.

De maneira geral, a Lei preza que os Dados Pessoais deverão ser utilizados apenas para as **finalidades específicas** para as quais foram coletados e **devidamente informadas aos titulares**, e, desta forma, **somente devem ser coletados os Dados mínimos necessários para que se possa atingir a respectiva finalidade**, e, após atingida a finalidade pela qual eles foram coletados, a LGPD determina a **imediata exclusão** dos Dados – excetuando casos em que a conservação é necessária para o cumprimento de obrigações legais ou regulatórias, por exemplo.

A QUEM SE APLICA?

A LGPD se aplica às pessoas físicas e jurídicas de direito público ou privado (abarcando, portanto, associações e sindicatos) que venham a realizar qualquer tipo de tratamento de Dados Pessoais, por meio físico ou digital, para fins econômicos. A LGPD não se aplica, por exemplo, ao tratamento de Dados Pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos ou realizado para fins jornalísticos, artísticos ou acadêmicos.

O QUE SIGNIFICA TRATAR UM DADO?

Assim como o conceito amplo a respeito dos Dados Pessoais, a LGPD apresenta um **conceito aberto** e um **rol exemplificativo** das ações que são consideradas como tratamento de Dados Pessoais. Ou seja, há a possibilidade de tratamento em ações/operações diversas das contempladas na Lei. Constituem, assim, 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.

Exemplos: o sindicato **acessa** uma planilha que contenha e-mail e endereço do associado, ou, ainda, **recebe** telefone para envio de informações institucionais, já há o tratamento de Dados Pessoais.

QUANDO POSSO TRATAR UM DADO?

A LGPD não é impeditiva quanto ao tratamento de Dados Pessoais, mas sempre é necessário ter um fundamento legal que autorize o referido tratamento, denominado pela LGPD como “Base Legal”.

Para a realização de tratamento de **Dados Pessoais** simples, temos a possibilidade de enquadramento em **10 (dez) bases legais taxativas** e elencadas no art. 7º da LGPD. Listaremos abaixo as Bases Legais previstas na Lei, destacando aquelas que melhor se enquadram nas principais atividades dos sindicatos, sem prejuízo da utilização das demais, quando aplicável:

• **(I) Consentimento do titular;** • **(II) Cumprimento de obrigação legal ou regulatória pelo Controlador;** • **(III) Pela administração pública para execução de políticas públicas;** • **(IV) Para a realização de estudos por órgãos de pesquisa;** • **(V) Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos Dados;** • **(VI) Para a proteção da vida ou incolumidade física do titular ou de terceiro;** • **(VII) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou por autoridade sanitária;** • **(VIII) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;** • **(IX) Quando necessário para atender aos interesses legítimos do Controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais;** e • **(X) Para a proteção do crédito.**

Dados Pessoais sensíveis, por sua vez, exigem maior cautela, de modo que a LGPD restringiu seu tratamento a somente 08 (oito) bases legais (elencadas no art. 11), **impedindo a utilização das bases legais do legítimo interesse e da proteção ao crédito para o tratamento de Dados sensíveis**. Além disso, podemos tratar um Dado Pessoal sensível, por exemplo, nas seguintes hipóteses:

- A garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos; e
- O exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral.

QUAIS OS PRINCÍPIOS QUE DEVEM SER OBSERVADOS NESSE TRATAMENTO?

A LGPD lista 10 (dez) princípios que devem ser levados em consideração em qualquer tratamento de Dados Pessoais, são eles:

Finalidade: A solicitação e tratamento de Dados Pessoais devem ser realizados com fins específicos, legítimos, explícitos e informados e não de forma genérica ou sem necessidade. Ou seja, deve-se explicar o motivo pelo qual os Dados Pessoais serão tratados. Não há mais a opção de se ter uma base de Dados para utilizar “quando e se precisar”, as finalidades devem ser definidas previamente ao início do tratamento dos Dados Pessoais. Assim:

- Pense se os Dados solicitados são realmente necessários;
- Questione o porquê requisitar certos Dados;
- Revise se há transparência suficiente fornecida aos titulares quanto ao uso dos seus Dados fornecidos e se há Base Legal que permita esse tratamento;
- Verifique se realmente utiliza os Dados que possui ou se você “tem só por ter”.

Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Exemplo: não se pode coletar nome e e-mail de colaboradores com a finalidade de realizar o cadastro nos sistemas internos do sindicato e readequar para outra finalidade, como o compartilhamento desses Dados a uma outra associação sem que haja prévia ciência do titular. Logo:

- Reveja se os Dados estão realmente sendo utilizados para o propósito definido ou para outras atividades não previstas também;
- Analise se a justificativa de uso do Dado é compatível ao Dado solicitado.

Exemplo: o associado preencheu formulário para realização de um evento X. A finalidade, portanto, é garantir sua participação no evento. O sindicato, assim, não pode utilizar esses Dados para finalidades diversas, como encaminhá-los para a equipe de comunicação realizar uma abordagem oferecendo demais serviços.

Necessidade: Utilizar os Dados estritamente necessários para alcançar as finalidades. A premissa de “menos é mais”.

- Pondere quais Dados são realmente necessários para a atividade realizada;
- Lembre-se que quanto mais Dados tratar, maior será a responsabilidade.

Livre Acesso: Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais.

- Encontre formas simples e acessíveis de o titular consultar seus Dados, como a elaboração de um aviso de privacidade, por exemplo, que conste no website do sindicato e indique quais Dados Pessoais são tratados, para qual finalidade, se são compartilhados com terceiros e qual o meio de comunicação (ex: criação de um e-mail) para que o titular exerça os seus direitos e comunique o Encarregado, se necessário.

- Disponibilize ao titular, de forma proativa e transparente, o que realiza com seus Dados, de que forma é realizado o tratamento e por quanto tempo.

Qualidade dos Dados: Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos Dados Pessoais.

- Tenha atenção à exatidão e relevância dos Dados Pessoais, de acordo com a finalidade de seu tratamento;
- Verifique se os Dados são verdadeiros, precisos e atualizados. Conforme previsto na LGPD, o titular tem o direito de correção de Dados incompletos, inexatos ou desatualizados.

Transparência: Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos Agentes de Tratamento. Refere-se ao “o que, porquê e para que” seus Dados estão sendo coletados e utilizados.

- Revise as informações passadas por seus meios de comunicação;
- Verifique se as informações são transmitidas com uma linguagem simples e de fácil entendimento;
- Não compartilhe os Dados Pessoais com terceiros de forma oculta, o titular deve estar sempre ciente de qualquer compartilhamento de suas informações.

Segurança: Utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

- Busque procedimentos e tecnologias que garantam a proteção dos Dados Pessoais de acessos por terceiros, a exemplo de processos de dupla autenticação e verificação da identidade, ferramentas de anonimização de Dados;
- Limite o acesso e tratamento de Dados a certos empregados.

Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais.

- Busque antecipadamente meios que garantam a proteção dos Dados Pessoais;
- Crie antecipadamente planos para solucionar situações acidentais que possam ocorrer, como a elaboração de documentos como o Plano de Resposta a Incidentes e Guia de Direito de Resposta aos titulares;
- É imprescindível revisar processos internos e promover a conscientização de pessoas de toda a organização para que vejam valor naquela atividade e os impactos da não observância.

Não Discriminação: Os Dados jamais podem ser tratados para fins discriminatórios ilícitos ou abusivos.

- Atente-se se possui Dados Pessoais – sejam eles sensíveis ou não - de titulares que podem gerar qualquer tipo de retaliação e discriminação.

Exemplo: Atestados médicos e exames ocupacionais dos colaboradores devem ser armazenados e acessados de modo restrito. A depender, se vazados, podem sujeitar o titular a situações vexatórias e constrangedoras.

Responsabilização e Prestação de Contas: Demonstração, pelo Agente de Tratamento, da 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.

- Acumule comprovações, como elaboração de políticas, registro das atividades Dados Pessoais, orientação e treinamento das equipes e utilização de protocolos que garantam a segurança dos Dados e demonstrem a boa-fé e o cuidado em permanecer em consonância com a LGPD.

1.2. LGPD E SINDICATOS

Diversos Dados Pessoais são tratados diariamente e registrados para o envio de comunicados, convites, informativos, cobranças de anuidade ou mensalidade, bem como outras atividades, portanto é fundamental que os sindicatos e associações tenham cuidado com a coleta, processamento e qualquer outro tratamento de Dados Pessoais não só de seus associados, mas de todos aqueles com quem se relacionam no exercício de suas atividades. Diante da nova legislação, é preciso cautela e atenção no compartilhamento de Dados Pessoais com empresas e entidades terceiras, seja por parcerias ou prestação de serviço. O consentimento específico para o fim de compartilhamento será peça-chave nestas situações para deixar clara ao titular a finalidade a qual seu dado pessoal se destina. Importante lembrar, no entanto, que só haverá necessidade de prévia concordância pelo titular se não for possível o enquadramento em outra Base Legal que permita o referido compartilhamento, a exemplo do envio de Dados Pessoais dos empregados ao E-Social, que decorre de uma obrigação prevista em Lei (Base Legal de cumprimento de obrigação legal ou regulatória).

Importante lembrar que: **Dados Pessoais relacionados à filiação a sindicato enquadram-se no conceito de Dados Pessoais sensíveis.** Devido ao seu teor e às consequências negativas e discriminatórias que seu vazamento pode causar ao titular, inclusive gerando direito à reparação moral tanto na esfera trabalhista quanto cível, a lei tratou de defini-los como “sensíveis” e prever tratamento especial, com bases legais inclusive mais restritivas.

Não seria possível, por exemplo, valer-se do legítimo interesse (Base Legal que pode ser aplicada para Dados Pessoais não sensíveis) para criar uma lista com os associados sindicalizados e sua filiação sindical e enviar convites e informações como reuniões, cursos, seminários, pesquisas, moções, buscas e outras formas de interações. Neste caso, a Base Legal mais pertinente seria a do consentimento, com a devida coleta de autorização, bem como com a opção de opt out (saída), a qualquer momento, pelo associado.

Por outro lado, sindicatos e associações podem, a exemplo, utilizar a Base Legal de exercício regular de direitos e, ainda, de obrigação legal ou regulatória para armazenar a relação dos nomes dos associados sindicalizados e respectivas Guias de Recolhimento de Contribuição Sindical (GRCSU) com vistas à representação de classe prevista pela Constituição Federal e para eventual salvaguarda quando do ajuizamento de eventual reclamação trabalhista. Diante da nova legislação, no tocante aos sindicatos e associações, **o olhar deve estar voltado a 3 (três) grupos principais, quais sejam (i) Colaboradores: Presidência, Diretoria, Gestores, Empregados do sindicato; (ii) Associados; e (iii) Terceiros**, de maneira geral: prestadores de serviços, fornecedores, parceiros de negócio e usuários de determinado website ou visitantes nas dependências do sindicato.

Assim, para **Colaboradores**, os Dados Pessoais poderão ser tratados em decorrência do contrato laboral firmado, por exemplo, ou para o cumprimento de obrigações legais e regulatórias (exemplo: informações transmitidas ao E-Social) ou, ainda, para permitir o exercício regular de direitos em caso do ajuizamento de reclamações trabalhistas. Para a transparência, recomenda-se a elaboração de um Aviso de Privacidade Interno e Políticas de Privacidade.

Quanto à relação com os **Associados**, devem receber total transparência a respeito de quais Dados Pessoais são coletados e tratados. Muitas das atividades sindicais são envios de comunicação, eventos, palestras, clubes de benefícios e a escolha pela adesão deve ser tratada de forma livre pelo Associado, nesses casos, o consentimento também parece ser a melhor opção para tratamento de Dados decorrentes de tais atividades.

Por fim, a relação com **Terceiros**, no caso em que houver o compartilhamento e tratamento de Dados Pessoais entre as Partes, os contratos devem conter cláusulas específicas para que se estabeleça os critérios e padrões mínimos para condução do tratamento e definição das responsabilidades entre os agentes. Para a transparência, recomenda-se também a elaboração de um Aviso de Privacidade Externo.

Vale lembrar que todo e qualquer tratamento envolvendo Dados Pessoais deve estar amparado por uma Base Legal e o consentimento é a única Base Legal que pode ser revogada a qualquer momento. Logo, caso o titular revogue o consentimento, deve-se analisar se (i) atingida a finalidade pretendida com o tratamento daquele Dado Pessoal (o que, em tese, gera a obrigação de não mais utilização) ou (ii) se solicitada a exclusão, por exemplo, pelo titular, há alguma outra Base Legal que ampare a continuidade desse tratamento. Ou, (iii) caso negativo, se é possível a anonimização desses Dados Pessoais. Se frustrada as etapas acima, a revogação deve ser concedida ao titular.

Nos próximos capítulos, estes e outros temas serão abordados com mais profundidade e detalhamento para melhor entendimento. Por ora, é importante compreender que é essencial adotar políticas de privacidade e proteção e utilizar conscientemente as informações dos Colaboradores, Terceiros e Associados de modo a fornecer-lhes diretrizes de boas práticas e máxima transparência.

1.3. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Estabelecida por meio da Lei 13.853/2019, a Autoridade Nacional de Proteção de Dados (ANPD) é o órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, bem como será encarregada de editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos para adequação.

É composta por um Conselho Diretor, Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas necessárias à aplicação da lei.

As **sanções administrativas**, poderão ser aplicadas **a partir de 1º de agosto de 2021**. As sanções serão aplicadas àqueles que descumprirem as disposições legais e por este motivo, mostra-se relevante a adequação das empresas ao disposto na Lei. É importante realizar a adequação perante a severidade das sanções, como:

Sanções administrativas (art. 52º): os Agentes de Tratamento de Dados, em razão das infrações cometidas às normas previstas na Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela Autoridade Nacional:

- (I) Advertência, com indicação de prazo para adoção de medidas corretivas;
- (II) 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;
- (III) Multa diária, observado o limite total a que se refere o inciso II;
- (IV) Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- (V) Bloqueio dos Dados Pessoais a que se refere a infração até a sua regularização;
- (VI) Eliminação dos Dados Pessoais a que se refere a infração;
- (VII) Suspensão parcial do funcionamento do banco de Dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo Controlador;
- (VIII) Suspensão do exercício da atividade de tratamento dos Dados Pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e
- (IX) Proibição parcial ou total do exercício de atividades relacionadas a tratamento de Dados.

Porém, importante ressaltar que, mesmo que as sanções administrativas só possam ser aplicadas pela ANPD a partir de 1º de agosto de 2021, como a LGPD já está em vigor, ações judiciais e indenizações já vêm sendo utilizadas com amparo nas disposições nela contempladas, exigindo dos Agentes de Tratamento imediata conformidade à legislação e seus princípios norteadores.

Nesse mesmo sentido, é válido pontuar que, quando estiverem em vigor, as sanções serão aplicadas após procedimento administrativo que possibilite defesa do agente, levando em conta os seguintes critérios: a gravidade e a natureza das infrações e dos direitos pessoais afetados, a **boa-fé** do infrator, possíveis vantagens econômicas auferidas pelo infrator, a condição econômica do infrator, a reincidência, o grau do dano, a **cooperação** para esclarecimento do caso, **demonstração de evidências de mecanismos, procedimento e adoção de boas práticas** de segurança para minimizar possíveis danos causados aos titulares, a pronta adoção de medidas corretivas, e a proporcionalidade entre a gravidade da falta e a intensidade da sanção. Importante observar que os mencionados critérios que serão considerados para a aplicação das penalidades reforçam ainda mais os impactos positivos para as entidades que se adequarem o quanto antes à LGPD.

NOTIFICAÇÕES DE INCIDENTES – QUANDO SÃO OBRIGATÓRIAS?

O **Controlador** deverá comunicar à ANPD e ao titular, dentro de prazo razoável, sobre a ocorrência de incidente de segurança envolvendo Dados Pessoais que possa acarretar risco ou dano relevante aos titulares, descrevendo aspectos como:

- (I) Descrição da natureza de Dados Pessoais afetados;
- (II) Informações sobre os titulares envolvidos;
- (III) A indicação de medidas técnicas e de segurança utilizadas para a proteção de Dados Pessoais;
- (IV) Os riscos relacionados ao incidente;
- (V) Os motivos da demora, no caso de a comunicação não ter sido imediata;
- (VI) Medidas adotadas ou que serão para reverter ou mitigar os prejuízos.

Até que haja regulamentação pela ANPD do “prazo de comunicação” e de demais aspectos relacionados a incidentes, na prática, as entidades, de maneira geral, devem:

- Adotar a postura de que **tão logo** (sendo tal considerado a título indicativo, pela ANPD, o **prazo de dois dias úteis**, contados da data do conhecimento do incidente) se tenha informações confiáveis sobre incidentes e sua entidade esteja apta a abordar os tópicos mencionados acima, a notificação e comunicação deva ser realizada;

Importante: preliminarmente, até a efetiva regulamentação, a ANPD já disponibilizou formulário de comunicação de incidente de segurança com Dados Pessoais, bem como documento que contém orientações sobre o que fazer em caso de um incidente. Tais documentos servirão como Guia enquanto não realizada a necessária regulamentação.

- Definir e classificar, em conjunto com o Encarregado de Dados, quais Dados Pessoais, se violados, acarretariam risco ou dano relevante aos titulares para que se opte pela comunicação ou não, para facilitar a verificação sobre a necessidade de comunicação de incidente à ANPD.
- Para saber mais sobre o que fazer em caso de um incidente de segurança com Dados Pessoais, acesse <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>.

GLOSSÁRIO EXEMPLIFICATIVO

GLOSSÁRIO EXEMPLIFICATIVO

Agentes de Tratamento: O Controlador e o Operador.

Anonimização: 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.

Banco de Dados: Conjunto estruturado de Dados Pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Consentimento: Manifestação da vontade livre, específica e explícita, nos termos em que o titular dos Dados aceita mediante ato positivo que seus Dados Pessoais sejam tratados.

- (I) Livre: deve ser conferido o poder de escolha de quais Dados fornecer e quais não fornecer, além de ser capaz de revogar o seu consentimento a qualquer momento;
- (II) Informado: devem ser fornecidas informações aos titulares dos Dados, como a identificação do Controlador e as finalidades para as quais o tratamento de Dados se destina; e
- (III) Inequívoco: requer a demonstrabilidade de que o titular consentiu com o tratamento de seus Dados.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de Dados Pessoais.

Dado Anonimizado: Aqueles que não são Dados Pessoais. Dado anonimizado é relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento.

Exemplo: Anonimização de Dados Pessoais de associados sindicalizados para fins de estudo e estatística. Originariamente, poderia ser relativo a uma pessoa, mas passou por etapas que garantiram a desvinculação do dado a essa pessoa em específico, de maneira a não mais identificá-la.

Dado Pessoal:

Exemplo: RG, CPF, nome, telefone, e-mail, endereço, data de nascimento, cargo, escolaridade, profissão, nacionalidade, interesses. (Esses exemplos não necessariamente serão Dados Pessoais, somente se passíveis de identificar ou tornar alguém identificável).

Informação relacionada a pessoa natural identificada ou identificável, ou seja, **qualquer Dado que possa permitir a identificação de uma pessoa natural. O pensamento guia para definir se um Dado é pessoal ou não deve ser o seguinte: esse Dado individualmente ou em conjunto com algum outro é capaz de identificar alguém ou tornar alguém identificável? Se sim, temos a definição de um Dado Pessoal, passível de proteção pela LGPD.**

Não são considerados Dados Pessoais aqueles relativos a uma pessoa jurídica, como CNPJ, razão social, endereço comercial, entre outros. Dados Pessoais de representantes legais e procuradores, por sua vez, se passíveis de identificá-los, devem ser tratados como Dados Pessoais.

Exemplo 2: A diretoria possui a relação dos números de matrícula dos colaboradores contratados para fins de

controle, os quais, por si só, não são capazes de identificar qualquer empregado. Contudo, se cruzado com a base de Dados do Departamento de Recursos Humanos, será possível a identificação do titular, tornando-se um Dado Pessoal (agregado). Já como Dados Pessoais diretos, podemos citar, por exemplo, RG, nome e e-mail do associado sindicalizado.

Dado Pessoal Sensível: É a informação relacionada a pessoa natural identificada ou identificável 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.

São considerados sensíveis já que exigem especial atenção, tendo em vista que, se violados, podem trazer um perigo de discriminação ou segurança ao seu titular.

Exemplo: O departamento de RH da organização armazena informações sobre a licença médica dos seus colaboradores. Ou então faz o controle de entrada e saída de seus colaboradores por meio de biometria digital.

Eliminação: Exclusão de Dado ou de conjunto de Dados armazenados em banco de Dados, independentemente do procedimento empregado.

Encarregado de Proteção de Dados (Data Protection Officer - DPO):

Pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares dos Dados e a ANPD.

Dentre as funções do DPO, destacam-se:

- (I) Recepcionar e atender demandas dos titulares de Dados;
- (II) Interagir com a Autoridade Nacional de Proteção de Dados; e
- (III) Orientar colaboradores quanto a práticas de privacidade e proteção de Dados.

Apesar da obrigação de nomeação do Encarregado ser, a princípio, do Controlador, considerando que essa relação é dinâmica, ou seja, a entidade pode ser Operadora em seu modelo de negócio, mas Controladora em relação aos seus colaboradores, até que haja regulamentação da ANPD nesse sentido, sugere-se a indicação de um Encarregado para qualquer organização que trate Dados Pessoais.

Incidente de segurança da informação envolvendo Dados Pessoais: Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, perda, alteração, divulgação ou acesso não autorizado a Dados Pessoais tratados.

Operador: Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome do Controlador.

Relatório de impacto à proteção de Dados Pessoais: Documentação do Controlador, que poderá ser solicitada pela Autoridade Nacional de Proteção de Dados, e deverá conter 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 prevenção e mitigação de risco.

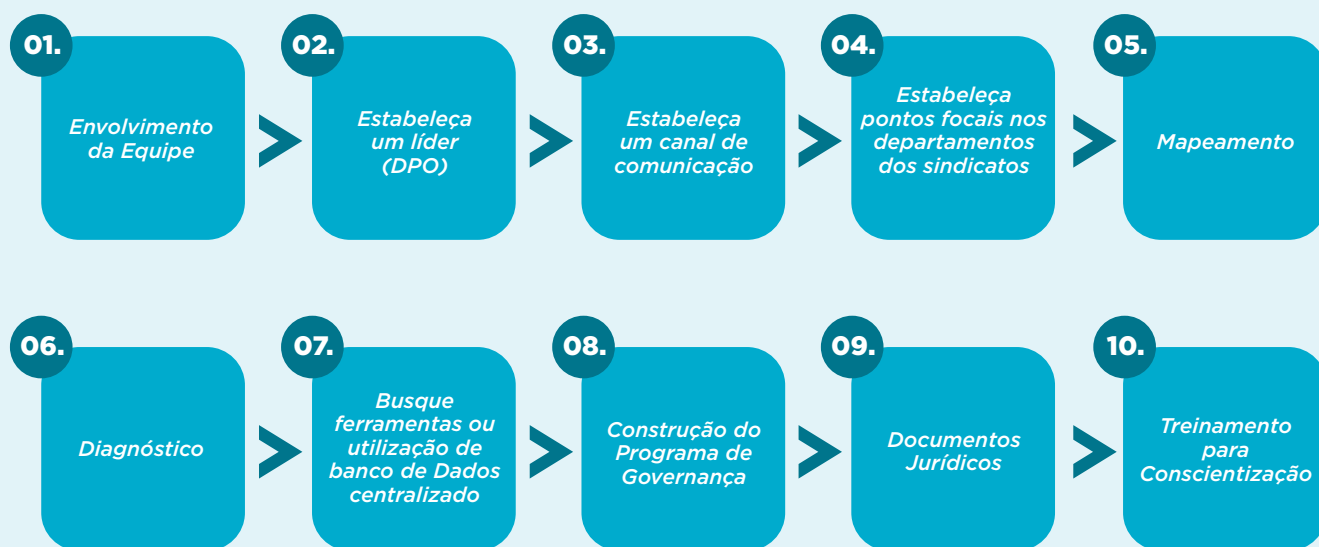
Titular: Pessoa natural a quem se referem os Dados Pessoais que são objeto de tratamento.

Violação de Dados Pessoais: Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, perda, alteração, divulgação ou acesso não autorizado a Dados Pessoais tratados.

PRINCIPAIS PASSOS PARA ADEQUAÇÃO

PRINCIPAIS PASSOS PARA ADEQUAÇÃO

Primeiramente, é importante que as organizações ponderem e levem em consideração em suas respectivas adequações, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de Dados que lhes competem.



3.1. ENVOLVIMENTO DA EQUIPE

Buscar o envolvimento dos executivos, da Diretoria, Conselho de Administração – se existente –, time jurídico, comercial, de Recursos Humanos, financeiro e todos aqueles que lidam diretamente com Dados Pessoais e possam ser afetados pela LGPD no exercício de suas atividades.

3.2. ESTABELEÇA UM LÍDER (ENCARREGADO - DPO)

O Encarregado pelo tratamento dos Dados Pessoais será o porta-voz do sindicato e centralizador de todas as ações necessárias à implementação de um projeto de adequação.

Logo, a identidade e informações de contato devem ser divulgadas publicamente, pelo website, por exemplo.

O Encarregado se reporta diretamente ao mais alto nível de direção e deve ser dotado de autonomia, estabilidade e independência orçamentária, sendo obrigatório, no momento, até regulamentação da ANPD nesse sentido, para todas as empresas e órgãos que tratam Dados Pessoais como Controladores, embora recomendável para qualquer organização.

QUEM PODE SER UM ENCARREGADO/DPO?

O Encarregado pode ser qualquer pessoa, inclusive jurídica ou até mesmo pessoa terceirizada alheia ao sindicato. Apesar de, até o momento, a Lei ser silente quanto a isso, recomenda-se que essa pessoa tenha a qualificação abaixo indicada.

A LGPD não impede que a função de Encarregado seja exercida em conjunto com outras funções dentro do sindicato. Contudo, é recomendável evitar que estas outras funções gerem **conflitos de interesse** com o papel esperado do Encarregado. Exemplo: este conflito pode surgir, por exemplo, da cumulação de cargos que realizam e/ou supervisionam muitos processamentos de Dados, os quais precisam ser auditados pelo Encarregado de forma imparcial.

QUAL QUALIFICAÇÃO O ENCARREGADO DEVE TER?

Recomenda-se que tenha, no mínimo, sólido conhecimento sobre:

- ✓ Lei Geral de Proteção de Dados;
- ✓ Regulamentações pertinentes às atividades do sindicato e que também se refiram à proteção de Dados;
- ✓ A natureza, o âmbito, o contexto e as finalidades das operações de tratamento de Dados realizadas pelo sindicato; e
- ✓ As necessidades específicas e desafios do sindicato no que tange à proteção de Dados.

Além das competências mínimas, há habilidades desejáveis, tais como:

- ✓ Saber interpretar normas e legislações, principalmente aquelas atreladas à privacidade e proteção de Dados Pessoais, incluindo noções do contexto legislativo internacional;
- ✓ Ter conhecimentos, no mínimo básicos, sobre tecnologia da informação e segurança da informação, além de entender as operações de tratamento de Dados Pessoais realizadas pelo sindicato; e
- ✓ Ter desenvoltura e boa comunicação para realizar a interação com diferentes áreas (inclusive com a alta liderança), bem como para lidar com o titular dos Dados e com a ANPD.

É NECESSÁRIO FORMALIZAR A POSSE DO ENCARREGADO?

Até o momento, a LGPD é silente quanto a isso. Porém, para fins de prestação de contas e accountability, recomenda-se que seja assinado um termo de confidencialidade, bem como realizado um termo de posse que indique (i) o nome do Encarregado, (ii) o período de mandato previsto; e (iii) e a responsabilidade e compromisso em assumir essa função. O documento deve ser datado e assinado pelo Encarregado e eventual membro do Conselho de Administração, de acordo com o requerido por Estatuto ou qualquer outro documento interno do sindicato.

Mesmo antes de qualquer formalização da pessoa do Encarregado, é importante e previsto na LGPD que já haja a criação de um canal de comunicação para contato com a referida disponibilização de preferência no website do sindicato.

3.3. ESTABELEÇA UM CANAL DE COMUNICAÇÃO

Fundamental para que se crie mecanismos tanto de (i) contato com o Encarregado quanto de (ii) exercício de direitos dos titulares.

A título de exemplo, os titulares dos Dados Pessoais podem solicitar a confirmação da existência de tratamento, a correção dos Dados inexatos ou a sua eliminação, assim como a informação sobre as entidades públicas ou privadas com as quais o Controlador possa ter compartilhado os Dados Pessoais daqueles, dentre outros direitos contemplados pela LGPD.

Na prática, um formulário no website pode ser disponibilizado ao titular para que preencha com as informações mínimas e necessárias para atendimento da solicitação e, ainda, que permita a correta validação de identidade do titular.

Para a correta validação da identidade do titular, pode-se solicitar, por exemplo, um e-mail para que se envie um link de confirmação ou, ainda, que se anexe no formulário de solicitação algum documento de identificação, como o RG, apto a comprovar a referida titularidade.

3.4. ESTABELEÇA PONTOS FOCAIS NOS DEPARTAMENTOS DOS SINDICATOS

Para que não haja a concentração de todo o trabalho nas mãos do Encarregado, se necessário, estabeleça pontos focais, sem poder de decisão, no entanto, dentro das organizações para auxiliarem no dia a dia das atividades de tratamento pessoal e disseminação de conhecimento e reporte ao Encarregado.

A criação de pontos focais, com reporte direto ao Encarregado, é importante para que o programa de governança seja contínuo e, principalmente, para que haja o registro e atualização, de forma constante, de todas as atividades de tratamento envolvendo Dados Pessoais em documento específico.

3.5. REÚNA INFORMAÇÕES SOBRE OS DADOS COLETADOS - MAPEAMENTO

A elaboração e a manutenção de um registro de tratamentos são elementos estruturantes da maior importância, sendo obrigatória a sua conservação para fins de controle interno, auditoria e fiscalização da ANPD.

Assim, saiba:

- Quais são os Dados Pessoais coletados;
- Como é o tratamento e qual a finalidade de cada tipo de Dados;
- Quando e como ocorre o fim do tratamento dos Dados;
- Como é realizado o compartilhamento dos Dados a terceiros;
- Qual o período de armazenamento e por qual razão.

Importante mencionar que a **base de Dados que já existia antes da vigência da LGPD** será ainda matéria de regulamentação pela ANPD, consideradas a complexidade das operações de tratamento e a natureza dos Dados. Ela também deve ser incluída na fase de mapeamento de Dados Pessoais, com um foco, inicialmente, àqueles Dados de maior criticidade para o sindicato, como os que exigem consentimento, por exemplo.

3.6. ANALISE SE OS DADOS ESTÃO SENDO TRATADOS CONFORME A LGPD - DIAGNÓSTICO

- Quais são Dados Pessoais e quais são sensíveis;
- Verifique se o tratamento e a respectiva Base Legal aplicada estão adequados ou não;
- Verifique se há consentimento do titular ou se há necessidade de nova coleta (caso a Base Legal mais adequada seja essa);
- Analise se o compartilhamento dos Dados está seguro e descrito em contrato, caso seja esse o cenário;
- Identifique os gaps e elabore uma matriz de risco, com identificação e classificação de riscos relativos aos Dados.

3.7. BUSQUE FERRAMENTAS OU UTILIZAÇÃO DE BANCO DE DADOS CENTRALIZADO

Suporte na definição de um sistema e/ou ferramentas que facilitem o monitoramento, gestão, registro das atividades e exclusão dos Dados Pessoais na organização.

A centralização de um banco de Dados facilita o atendimento às solicitações dos titulares e, se necessário, da própria ANPD.

3.8. CONSTRUÇÃO DO PROGRAMA DE GOVERNANÇA

Crie um programa de governança em proteção de Dados com a elaboração de medidas e controles para o acompanhamento da implantação de padrões que estejam em conformidade com a LGPD e legislações setoriais aplicáveis, especialmente que:

- Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos Dados tratados;
- Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- Tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

- Aplique mecanismos de supervisão internos e externos;
- Conte com planos de resposta a incidentes e remediação; e
- Seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

3.9. DOCUMENTOS JURÍDICOS

Elabore e revise documentos jurídicos, como avisos, políticas e procedimentos de privacidade na relação com o titular dos Dados e contratos com terceiros, a serem observados por todos da organização e por aqueles com quem ela se relaciona e que tenha o tratamento e/ou compartilhamento de Dados Pessoais.

- **Adeque contratos com terceiros** em que há o compartilhamento e tratamento de Dados Pessoais, inserindo e definindo as responsabilidades de cada Agente de Tratamento.

Vale lembrar que a LGPD responsabiliza todos os Agentes de Tratamento pela segurança e garantia da integridade dos Dados Pessoais que tratam, sendo que o Operador pode ser considerado solidariamente responsável com o Controlador caso descumpra a LGPD ou deixe de seguir as instruções lícitas instituídas por esse último. A relação entre os Agentes de Tratamento, portanto, deve ser delimitada em instrumento contratual adequado.

- Inclua disposição atinente à privacidade e proteção de Dados no **Código de Ética e Conduta** do sindicato, quando existente, tendo em vista a aplicabilidade das disposições ali dispostas aos colaboradores e associados, principalmente. Para os sindicatos que não possuem este documento, sem prejuízo, recomenda-se que seja instituída uma Política Geral de Privacidade e Proteção de Dados Pessoais, que determine a observância dos procedimentos internos (ex: manuseio e coleta dos Dados Pessoais) por todos do sindicato e por aqueles com quem ele se relacione e que tenha interação com Dados Pessoais. Para ambos os documentos, um termo de ciência pode ser assinado.

Lembrando que para a relação com terceiros (ex: prestadores de serviços, parceiros de negócio) em que há o tratamento de Dados Pessoais, cláusulas específicas devem ser inseridas no contrato.

- Dentre as **políticas, procedimentos e avisos**, destacam-se: (i) Aviso de Privacidade Interno, destinado aos colaboradores; (ii) Aviso de Privacidade Externo, a ser inserido no website para associados, terceiros e visitantes da página; (iii) Política Geral de Privacidade e Proteção de Dados Pessoais; e (iv) Política de Compartilhamento de Dados Pessoais.

3.10. TREINAMENTO PARA CONSCIENTIZAÇÃO

Realize treinamentos internos ou reuniões para alinhamento e apresentação das novas políticas/diretrizes de proteção de Dados Pessoais, visando a disseminação da cultura organizacional sobre o tema, bem como a equalização do tratamento de Dados por todos em sua entidade.

Assim, o respeito à LGPD só será atingido quando houver uma compreensão e conscientização pelos responsáveis por sua aplicação.

The background is a dark blue gradient with a network of thin, light blue lines and dots, creating a sense of connectivity and flow.

RELAÇÕES DE TRABALHO

4. COMO SE ADEQUAR:

Passemos agora para um passo a passo mais específico em relação ao tratamento de Dados Pessoais pelo sindicato quando do exercício de atividades nas relações **(i) de trabalho** (ex: colaboradores); **(ii) institucionais** (ex: associados, sindicalizados e parceiros de negócio) e **(iii) administrativas** (ex: diretores, representantes legais e terceiros prestadores de serviços).

4.1. RELAÇÕES DE TRABALHO

Sem coletar, receber, armazenar e reter Dados Pessoais de empregados ou candidatos a empregos, uma eventual relação de trabalho não poderia começar e se desenvolver. Desta forma, deve-se ter cautela e atenção quanto à aplicação da LGPD nas relações de trabalho, seja na etapa de seleção e recrutamento seja durante o processo de admissão do candidato ou até mesmo após eventual desligamento, a se considerar:

Fase pré-contratual – compreende todo o processo de seleção, ou seja, abertura da vaga, recebimento de currículos, até a efetiva contratação.

- Não deve haver discriminação com base em Dados Pessoais durante o processo de seleção;
- Apenas os Dados Pessoais necessários para a avaliação e seleção do candidato devem ser solicitados;
- Disponibilizar informações sobre o tratamento de Dados Pessoais através do **Aviso de Privacidade**.

Fase Contratual – inicia-se com a admissão do empregado e formalização de contrato.

- Atente-se às Bases Legais para o tratamento dos Dados Pessoais;
- O empregado deve ser informado sobre o tratamento de seus Dados Pessoais através do Aviso de Privacidade Interno, destinado aos colaboradores. Ainda, se aplicável, é importante que haja a leitura e ciência do Código de Ética e Conduta e procedimentos internos relacionados à privacidade;
- Tenha cautela na transferência de Dados Pessoais do empregado a terceiros (exemplo: plano de saúde).

Fase pós-contratual - é caracterizada pelo desligamento do empregado.

- Em sua maioria, haverá a necessidade de armazenamento de Dados Pessoais, mesmo após o desligamento, para fins de defesa no caso de ajuizamento de ações judiciais;
- Sugere-se a realização de uma **Tabela de Temporalidade** que contemple os prazos de guarda.

Para as relações trabalhistas, tenha sempre em mente os princípios da LGPD, listados no item 1.1 deste Guia, bem como o enquadramento da atividade em uma Base Legal que autorize o tratamento dos Dados Pessoais desses candidatos/empregados.

4.1.1. DADOS PESSOAIS TRATADOS NOS PROCESSOS DA RELAÇÃO DE TRABALHO

É fundamental compreender que o recebimento, inclusive por meio físico, de currículos que contenham Dados Pessoais dos candidatos, é uma forma de tratamento sujeita à aplicação da LGPD. Assim, desde o início, todo o tratamento decorrente da etapa de recrutamento e eventual admissão deve ser informado de forma clara e transparente a todos os candidatos que desejam participar de processos de seleção às vagas disponíveis.

QUAIS DADOS PESSOAIS PODEM SER SOLICITADOS PARA O RECRUTAMENTO E CONTRATAÇÃO? E QUAIS NÃO SÃO NECESSÁRIOS POR SEREM SENSÍVEIS?

Lembre-se sempre: candidatos são proprietários de seus Dados.

O início de um processo seletivo já conta com a disponibilização pelo candidato de Dados Pessoais à entidade, a exemplo do fornecimento de nome, endereço residencial, documentos de identificação e telefone. A implementação da LGPD tem como objetivo proteger esses Dados.

Contudo, a LGPD não prevê a descrição de quais Dados Pessoais podem ser solicitados em um processo seletivo e eventual contratação, de maneira que podem variar a depender das características e necessidades requeridas para aquela posição. As finalidades e informações acerca deste tratamento devem estar disponíveis de maneira clara ao titular, assim como deve se ter em mente que o recrutador deve obter apenas o mínimo necessário.

Há a intenção de coletar Dados sensíveis? Veja se, de fato, é necessário. Muitas das vezes o recrutador pode obter a informação que precisa sem que seja necessário o tratamento de Dados Pessoais sensíveis, uma vez que estes podem resultar em discriminação ao titular. O setor de Recursos Humanos ou o responsável pelo recrutamento deve ter cautela para não solicitar Dados Pessoais que não sejam relevantes para o processo de seleção.

Exemplo: há a intenção de contratar candidato que trabalhe aos sábados. Por mais que em algumas vezes através da pergunta de religião (Dado Pessoal Sensível) seja possível filtrar candidatos que não podem trabalhar aos sábados por motivos de crença, esse Dado exige cautela, podendo gerar, inclusive, potencial discriminatório desse candidato. Dessa forma, se perguntássemos simplesmente: “você tem disponibilidade de trabalhar aos sábados?”, obteríamos a informação pretendida, sem o tratamento de Dados Pessoais Sensíveis, no entanto. Portanto, reflita quais Dados Pessoais são realmente necessários e adequados para aquela seleção. Do contrário, não os solicite.

Sobre Dados Pessoais de saúde: a realização de exames periódicos durante a fase de contratação e durante o período da relação de trabalho costumam encontrar respaldo na legislação vigente (é importante, porém, verificar se, de fato, há respaldo em Lei para que haja o enquadramento dessa atividade de tratamento na Base Legal mais adequada). Contudo, não podem ser solicitados exames que possam expor a saúde do trabalhador a fim de causar-lhe discriminação, a exemplo dos exames de HIV, gravidez, câncer etc.

Sugere-se, portanto, informar ao titular, através do **Aviso de Privacidade** disponibilizado no website:

- O tratamento que será realizado com os Dados Pessoais fornecidos;

- Por quanto tempo essas informações ficarão armazenadas no banco de vagas (nesse cenário, há a possibilidade de enquadramento na Base Legal de exercício regular de direitos durante o prazo prescricional, caso o candidato ajuíze ação judicial alegando, por exemplo, discriminação durante o processo seletivo). Após, se não autorizado pelo candidato ou se não houver nenhuma outra Base Legal que justifique o tratamento, os Dados Pessoais deverão ser descartados ou anonimizados, nas hipóteses autorizadas por Lei;
- Se haverá compartilhamento com empresa terceira e, caso haja, que se verifique se há Base Legal autorizada para tanto. Se a atividade de tratamento estiver fundamentada no consentimento, outro consentimento deverá ser obtido de maneira específica para esse compartilhamento;
- Deixar clara a utilização desses Dados estritamente para a candidatura da vaga anunciada. Exemplo: esses Dados Pessoais não poderão ser utilizados para o envio de convites para palestras e cursos.

COMO MANTER E O QUE FAZER COM AS INFORMAÇÕES CONTIDAS NO CURRÍCULO DURANTE TODO O PROCESSO DE SELEÇÃO?

É necessário definir empregados autorizados e aptos a manusear esses Dados Pessoais dentro do sindicato, bem como um local adequado para armazenamento dessas informações, criando-se, assim, um manuseio seguro e em consonância com a Lei.

Seja transparente e detalhe aos candidatos as práticas e utilização dos Dados Pessoais coletados, através do **Aviso de Privacidade** disponibilizado no website.

Também é necessário documentar a autorização de uso, se o consentimento for a Base Legal mais adequada para o tratamento de determinado Dado Pessoal. Neste caso, deve-se fazer uma gestão desse consentimento para que se garanta o atendimento aos direitos dos titulares se solicitado, a exemplo da possibilidade de revogação.

HÁ NECESSIDADE DE QUE OS CANDIDATOS EXPRESSEM O CONSENTIMENTO EM OFERECER OS SEUS DADOS PESSOAIS PARA O SINDICATO, PERMITINDO SUA UTILIZAÇÃO E ARMAZENAMENTO?

A obtenção do consentimento só será necessária se não for possível que o sindicato enquadre o referido tratamento em Base Legal diversa e a depender de cada situação.

De toda forma, **durante a fase de recrutamento e seleção**, considerando que ainda não há uma expectativa do candidato em ser selecionado, a Base Legal mais adequada será a do consentimento e, em alguns casos, a depender da finalidade e da categoria de Dados Pessoais tratados – se sensíveis ou não – a de legítimo interesse (para Dados Pessoais Sensíveis, o legítimo interesse não poderá ser utilizado) do sindicato também poderá ser utilizada.

Ao ser **admitido no processo seletivo e ao dar início à etapa de contratação do candidato, é importante que o sindicato tenha em mente o seguinte:** considerando existir um desequilíbrio entre empregado e empregador, o consentimento como Base Legal deve ser utilizado apenas como última alternativa, já que ao pedir o consentimento para o tratamento de Dados Pessoais na relação empregatícia, o empregado, na realidade, pode não consentir de forma totalmente livre, como determina a LGPD. Ao contrário, o empregado pode sentir-se constrangido a consentir, sob pena de ser desligado, por exemplo, ou não dar continuidade ao seu processo de admissão.

Exemplo: a coleta da biometria do empregado para fins de gestão de ponto não pode estar associada ao consentimento do empregado. Isto porque, caso ele não autorize a coleta, não haverá como fazer a marcação do seu ponto e garantir-lhe o devido recebimento de salário. Neste sentido, o consentimento do empregado não seria livre, por não haver opção, uma vez que a coleta, neste caso, é compulsória e inerente ao contrato de trabalho, sendo a execução do contrato a Base Legal mais adequada e não o consentimento.

Ainda, importante ressaltar que, caso seja necessário o compartilhamento desses Dados Pessoais com outras empresas recrutadoras, por exemplo, se o sindicato utilizou o consentimento como Base Legal para tratar esses Dados Pessoais, também deverá obter consentimento específico do titular para o fim de compartilhamento. Neste caso, a coleta do consentimento tanto para o tratamento da atividade em si (Exemplo: ``seleção de currículos) quanto para o compartilhamento dos Dados Pessoais com empresa terceira pode estar no mesmo documento, porém, deve haver solicitação específica (em item apartado) para o compartilhamento em si, podendo o titular concedê-lo ou não.

Em um outro cenário, se o compartilhamento for realizado para cumprir determinada obrigação legal, por exemplo, a obtenção do consentimento não será necessária, já que estamos em uma hipótese de enquadramento em Base Legal diversa, que dispensa a necessidade do consentimento.

COMO DEVO PROCEDER EM RELAÇÃO AO CANDIDATO SOBRE O USO DE SEUS DADOS PESSOAIS?

Em relação ao candidato à vaga, como já pontuado, é importante, desde o início, a disponibilização de um Aviso de Privacidade que conste informações acerca do tratamento de seus Dados Pessoais.

Quando selecionado, é válido pontuar que, nessa fase, o candidato já tem a expectativa de contratação, de modo que, de maneira geral, quando o Dado Pessoal não for sensível, as Bases Legais que podem ser utilizadas, a depender do caso, serão a da execução de contrato (exemplo: biometria), cumprimento de obrigação legal ou regulatória (exemplo: envio de informações ao E-Social) e exercício regular de direitos (exemplo: caso seja ajuizada alguma ação judicial pelo empregado).

No caso de Dados Pessoais Sensíveis, é importante cautela na coleta e enquadramento na Base Legal mais adequada. Assim, deve-se verificar se o tratamento é necessário para o cumprimento de alguma obrigação legal, por exemplo, como as vagas destinadas para PCDs, ou se será utilizada outra Base Legal.

Caso o candidato seja admitido, ao integrar o sindicato, é aconselhável que, dentre os treinamentos a serem realizados, conste o relativo à Política de Privacidade e Proteção de Dados Pessoais, reforçando, inclusive, a leitura do Aviso de Privacidade Interno (destinado aos colaboradores) e seu local de armazenamento. Ainda, o candidato deve ser informado sobre a existência de um canal de comunicação, caso queira exercer seus direitos, bem como da figura do Encarregado, se existente qualquer dúvida.

Já em relação aos **candidatos que não forem contratados**, recomenda-se o armazenamento dos Dados Pessoais e do processo de seleção pelo prazo prescricional (como regra na esfera trabalhista é o de 5 (cinco) anos) referente a eventual ajuizamento de ação judicial por esse candidato que pode, por exemplo, alegar possível discriminação durante a fase de recrutamento. Neste caso, a Base Legal pertinente para o armazenamento será a de exercício regular de direitos. Após transcorrido esse prazo, caso não haja Base Legal que justifique a continuidade desse tratamento pelo sindicato, as informações devem ser excluídas ou anonimizadas, caso aplicável. Ressalta-se que os prazos prescricionais devem ser constantemente verificados junto ao departamento jurídico/Encarregado, a depender da situação em concreto, para melhor definição.

Dica! Importante comentar que, no caso de entrevista realizada por videoconferência, considerando haver também o tratamento Dados Pessoais, inclusive sensíveis e aspectos relacionados à imagem e voz do candidato, recomenda-se a adoção de especial cautela, especialmente quando há a intenção de armazenamento desses vídeos.

É NECESSÁRIO ALGUM AJUSTE NO CONTRATO DE TRABALHO?

Inicialmente, é importante que o empregado, ao entrar no sindicato, tenha acesso tanto à Política Geral de Privacidade e Proteção de Dados, Código de Ética e Conduta, quanto ao Aviso de Privacidade Interno (destinado aos colaboradores) contendo informações do tratamento de seus Dados Pessoais.

Ao ler esses documentos, recomenda-se a assinatura de um **Termo de Ciência** para que o colaborador saiba dos procedimentos internos da entidade que devem ser cumpridos, como também a maneira como deve tratar os Dados Pessoais no exercício de suas atividades cotidianas. Um exemplo de redação do Termo de Ciência pode ser o vislumbrado abaixo:

“Eu, (nome do empregado), matrícula X e CPF/RG nº X, declaro, para os devidos fins, que tenho total conhecimento da existência e do conteúdo do Código de Ética e Conduta/Política Geral de Privacidade e Proteção de Dados Pessoais e demais procedimentos internos do (incluir nome do sindicato), e que estes passam a fazer parte integrante do meu Contrato de Trabalho.

Estou ciente de que a não observância dos documentos listados acima poderão implicar na caracterização de falta grave, que poderá ser passível de aplicação de medidas administrativas e legais cabíveis, tanto na esfera cível e trabalhista quanto criminal.”

Local e Data

Assinatura

Considerando o desequilíbrio entre empregado e empregador abordado em tópico anterior, recomenda-se que o consentimento seja utilizado, preferencialmente, apenas nos casos estritamente mandatórios por Lei ou quando for impossível a aplicação de outra Base Legal ou, ainda, para adesão de algum benefício que, de fato, possa ser escolhido livremente pelo empregado. Nos casos em que a coleta de consentimento for realmente necessária para o tratamento de atividade específica, sugere-se a realização de termo apartado ao contrato de trabalho. Um exemplo de consentimento obrigatório pela LGPD é quando há o tratamento de Dados Pessoais de criança, que exigem o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

OS DADOS PODEM SER ARMAZENADOS EM UM BANCO DE TALENTOS/BASE DE DADOS?

A aplicação da LGPD tem um impacto direto na manutenção dos bancos de currículos, uma vez que devem ser mantidos somente por um determinado período.

A prática de coleta e geração do banco de currículos deve ser aprimorada. Os sindicatos que ainda dependem do RH tradicional e tendem a arquivar documentos em papel para análise de recrutamento podem sofrer mais com a LGPD. É interessante, se este for o caso, pensar na automatização do processo, para facilitar essa gestão e torná-lo mais seguro, inclusive se o titular quiser exercer algum de seus direitos.

Ademais, lembre-se que o consentimento pode ser necessário caso não haja outra Base Legal que autorize o armazenamento de Dados dos candidatos. Exemplo, num cenário em que a guarda de Dados foi feita para fins de exercício regular de direitos, quando esgotar o prazo prescricional de ajuizamento de uma demanda judicial e não houver outra Base Legal, somente será possível manter as informações na base de Dados/banco de talentos mediante o consentimento específico do titular, do contrário, deverá ser feita a exclusão ou anonimização dessas informações, se aplicável.

Ainda, é de extrema importância que no Aviso de Privacidade conste por quanto tempo essas informações ficarão armazenadas no banco de vagas/Base de Dados (nesse cenário, há a possibilidade de enquadramento na Base Legal de exercício regular de direitos durante o prazo prescricional, caso o candidato ajuíze ação judicial alegando, por exemplo, discriminação durante o processo seletivo). Após o fim do prazo prescricional, **se não autorizado pelo candidato ou se não houver nenhuma outra Base Legal** que justifique o armazenamento, os Dados Pessoais deverão ser descartados.

APÓS O TÉRMINO DO VÍNCULO EMPREGATÍCIO, QUAL A ORIENTAÇÃO SOBRE OS DADOS PESSOAIS ARMAZENADOS, COMO GERENCIAR OS DADOS DOS ANTIGOS EMPREGADOS?

Após o término do vínculo empregatício, recomenda-se a exclusão ou anonimização de todos os Dados Pessoais cujo armazenamento não seja obrigatório. Desta forma, a entidade se protege contra possíveis falhas ou vazamentos.

Porém, é válido pontuar que, de maneira geral, documentos previdenciários e trabalhistas (contrato de trabalho, rescisão, aviso prévio, dentre outros), podem permanecer armazenados na entidade para cumprimento de

obrigações legais ou regulatórias pelo tempo exigido pela legislação aplicável. É possível, ainda, que a entidade continue armazenando os Dados do empregado mesmo após sua demissão visando defender-se em eventual demanda judicial, administrativa ou arbitral (Base Legal de exercício regular de direitos).

Neste sentido, sugere-se a realização de uma **Tabela de Temporalidade**, documento esse que contemplará os prazos de guarda, decorrentes de Lei ou Normas Regulamentadoras, para auxílio do Encarregado quanto ao armazenamento ou exclusão dos Dados Pessoais dos empregados. Importante ressaltar que a Lei é esparsa e muitas vezes pouco orientativa em relação a esses prazos, exigindo-se especial cautela nessa definição. Válido ter em mente que, embora a Tabela de Temporalidade sirva com um guia ao Encarregado dos documentos que devem ser mantidos no sindicato considerando-se o prazo de guarda previsto em Lei ou Normas Regulamentadoras, a cultura a ser adotada é a de que os Dados Pessoais só devem ser armazenados pelo tempo mínimo necessário para que seja cumprida a finalidade que justifica o seu tratamento, seja ela legal ou não.

A **Tabela de Temporalidade** poderá conter informações como:

- Categoria (Exemplo: trabalhista);
- Documento (Exemplo: livro de salários);
- Período de retenção (Exemplo: 10 anos);
- Fundamentação legal (Exemplo: 13.146/2015);
- Comentários.

Veja alguns prazos trabalhistas a serem considerados e que podem servir de base para criação de uma tabela de temporalidade:

DOCUMENTO	PRAZO	FUNDAMENTO LEGAL
FGTS – FUNDO DE GARANTIA DO TEMPO DE SERVIÇO	5 anos	Art. 7º, XXIX, CF e art. 11 CL
CONTRIBUIÇÃO SINDICAL – GRCSU	5 anos	Arts. 174 e 217, I, CTN
CONTRATO DE TRABALHO	–	Indeterminado
LIVRO OU FICHA DE REGISTRO DE EMPREGADO	–	Indeterminado
RECIBO DE PAGAMENTO DE SALÁRIO, FÉRIAS, 13º SALÁRIO E CONTROLE DE PONTO	5 anos	Art. 7º, XXIX, CF e art. 11 CLT
TERMO DE RESCISÃO DO CONTRATO DE TRABALHO, PEDIDO DE DEMISSÃO E AVISO PRÉVIO	2 anos	Art. 7º, XXIX, CF e art. 11 CLT
FOLHA DE PAGAMENTO	10 anos	Art. 225, I e § 5º, decreto n.º 3.048/1999
RAIS – RELAÇÃO ANUAL DE INFORMAÇÕES SOCIAIS	5 anos	Art. 8º, Portaria MTB n.º 1.464/2016

4.1.2. TRANSMISSÃO DE DADOS PESSOAIS DECORRENTES DA RELAÇÃO DE TRABALHO A TERCEIROS

COMO MINISTRAR A RELAÇÃO DESSAS INFORMAÇÕES OBTIDAS E COMO OS DADOS PODEM SER TRANSFERIDOS?

Lembre-se sempre do princípio da finalidade: os Dados Pessoais obtidos devem ter uma justificativa e ser utilizados para um fim específico.

A transparência ao titular vem em primeiro lugar, portanto, atente-se em informar ao titular sobre o tratamento e transferência/compartilhamento de seus Dados Pessoais, para quais empresas – se aplicável – e para qual finalidade e, se necessário, colete o devido consentimento para que os Dados sejam transferidos a terceiros.

Ainda, importante lembrar que, sendo um dos direitos de os titulares obter a informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de Dados, o sindicato deve manter essa relação mapeada no seu documento de registro das atividades envolvendo Dados Pessoais dentro do sindicato.

De toda maneira, em um primeiro momento, o Aviso de Privacidade pode abarcar essas entidades de forma categorizada por grupos (exemplo: instituições financeiras, operadoras de saúde), ou seja, a priori, não se faz necessário listar todas as empresas com as quais há o referido compartilhado. Porém, caso solicitado pelo titular, deverá o sindicato fornecer a relação em detalhes.

COMO FAÇO PARA ENVIAR DADOS PESSOAIS DE EMPREGADOS A EMPRESAS TERCEIRAS? (EX. PRESTADORES DE SERVIÇOS, VR, CONVÊNIO...)

Inicialmente, é válido ter em mente se a concessão do benefício decorre de uma obrigação legal (Exemplo: vale-transporte) ou, ainda, de estipulações tratadas em acordos ou convenções coletivas (Exemplo: concessão de vale-refeição), de modo que, nesses casos, a Base Legal que autorizará o tratamento não será a do consentimento, mas sim a de obrigação legal ou regulatória.

Muitas vezes, também, os benefícios concedidos já estão contemplados no próprio contrato de trabalho do empregado, de modo que, nesses casos, teremos o enquadramento na Base Legal de execução de contrato ou exercício regular de direitos em contrato, este último quando tratados Dados sensíveis.

Caso não enquadrados em nenhuma das hipóteses acima, esses Dados Pessoais poderão ser tratados com base na coleta de consentimento ou, ainda, no legítimo interesse (para Dados Pessoais Sensíveis, o legítimo interesse não poderá ser utilizado).

Importante ressaltar que sempre quando houver o compartilhamento de Dados Pessoais com terceiros, as cláusulas contratuais devem estar ajustadas de modo a definir as responsabilidades dos agentes e garantir um tratamento adequado e de acordo com a LGPD. Ainda, se utilizada a Base Legal de consentimento, um consentimento específico para esse compartilhamento também deverá ser coletado.

Por sua vez, se o compartilhamento for realizado para cumprir determinada obrigação legal, por exemplo, a obtenção do consentimento não será necessária, já que estamos em uma hipótese de enquadramento em Base Legal diversa, que dispensa a necessidade do consentimento.

Ainda, especificamente no que tange à coleta de Dados Pessoais de dependentes menores de 12 anos incompletos, o consentimento deve ser, obrigatoriamente, por um dos pais ou responsáveis legais de maneira específica e em destaque.

As informações relativas a esses tratamentos deverão estar abarcadas no Aviso de Privacidade Interno, destinado aos colaboradores.



DEPARTAMENTO
DE DEFESA E SEGURANÇA

FICHA TÉCNICA

ELABORAÇÃO

Rony Vainzof

Diretor do Departamento de Defesa e Segurança da FIESP e
Coordenador do Grupo de Trabalho de Segurança e Defesa Cibernética

Luciana Nunes Freire

Diretora Executiva Jurídica da FIESP

Larissa Nunes Silva

Analista do Departamento de Defesa e Segurança da FIESP

Maria Eduarda Annarumma Guedes

Colaboradora do Grupo de Trabalho de Segurança e Defesa Cibernética

COORDENAÇÃO

Luciano Villela Coelho

Gerente do Departamento de Defesa e Segurança da FIESP

APOIO

Adriana Carletti Fonseca

Gerente do Departamento Sindical e de Serviços da FIESP | Divisão de Serviços

Amanda Alves de Melo

Assistente Administrativa do Departamento Sindical e de Serviços da FIESP |
Divisão de Serviços

SINDICOURO

Sindicato da Indústria do Curtimento de Couros e Peles no Estado de São Paulo

SIETEX

Sindicato das Indústrias de Especialidades Têxteis no Estado de São Paulo

SINDIMOV

Sindicato da Indústria do Mobiliário de São Paulo

FIESP CIESP