FIESP | DEPARTAMENTO DE DEFESA E SEGURANÇA

GUIA ORIENTATIVO ÀS EMPRESAS

LGPD - LEI GERAL DE PROTEÇÃO DE DADOS

São Paulo, maio de 2022.

FIESP CIESP

A Federação das Indústrias do Estado de São Paulo (FIESP) e o Centro das Indústrias do Estado de São Paulo (CIESP) apresentam o Guia LGPD às Empresas, um complemento à Cartilha de Proteção de Dados Pessoais. O Guia traz orientações objetivas e informações sobre a Lei Geral de Proteção de Dados Pessoais (LGPD) para que toda e qualquer entidade que esteja sujeita à aplicação da legislação possa ter em mãos uma importante ferramenta para seguir na contínua jornada de adequação e conformidade.

Diante dos diversos desafios para a implementação da LGPD, a FIESP e o CIESP têm realizado, com muito orgulho e dedicação, um imenso esforço para auxiliar nossas empresas e sindicatos nesta trilha de conformidade, 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 nos debruçado de forma profunda sobre o tema da Segurança e Defesa Cibernética e da Proteção de Dados, promovendo conhecimento para toda a sociedade. Agora, com a vigência e amadurecimento 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 as indústrias e a sociedade brasileira

---

Federação das Indústrias do Estado de São Paulo – **FIESP**
Centro das Indústrias do Estado de São Paulo – **CIESP**

INTRODUÇÃO

Com a aprovação em 2018 da Lei Geral de Proteção de Dados Pessoais (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. É neste mesmo sentido que houve a promulgação, em fevereiro de 2022, da Emenda Constitucional nº 115, de maneira a consolidar este entendimento a partir da inclusão na Constituição Federal brasileira da garantia à proteção de Dados Pessoais entre os direitos e garantias fundamentais do indivíduo, bem como do estabelecimento da competência privativa da União para legislar sobre o tema.

Com a intenção de apoiar as empresas no uso e 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 empresarial.

As informações disponíveis no Guia são sobre a LGPD e a ANPD, principais passos para o início do processo de conformidade, como adequar as relações de trabalho, comerciais e administrativas, e especificidades da aplicação da Lei à micro e pequenas empresas, startups e pessoas físicas que realizam tratamento de Dados para fins econômicos. Há ainda um FAQ com as principais dúvidas.

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

PROPOSTA

- Um Guia Orientativo, exemplificativo e acessível ao dia a dia empresarial;
- Direitos fundamentais dos titulares dos dados (Legislação);
- Penalidades pelo não cumprimento da Lei;
- Consolidação de alguns conceitos com exemplificação;
- Direcionamento para início do processo de conformidade/adequação à LGPD;
- Orientação quanto à adequação de procedimentos e documentos.

ÍNDICE

1. LEGISLAÇÃO **6**
1.1 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS 7
1.2 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E AS SANÇÕES 11
1.3 LGPD E EMPRESAS 14
2. GLOSSÁRIO EXEMPLIFICATIVO **16**
3. PRINCIPAIS PASSOS PARA O INÍCIO DO PROCESSO DE ADEQUAÇÃO/CONFORMIDADE **20**
3.1 ENVOLVIMENTO DA EQUIPE 22
3.2 ESTABELEÇA UM LÍDER (ENCARREGADO - DPO) 22
3.3 ESTABELEÇA UM CANAL DE COMUNICAÇÃO 23
3.4 ESTABELEÇA PONTOS FOCAIS NOS DEPARTAMENTOS 24
3.5 REÚNA INFORMAÇÕES SOBRE OS DADOS COLETADOS - MAPEAMENTO 24
3.6 ANALISE SE OS DADOS ESTÃO SENDO TRATADOS CONFORME A LGPD - DIAGNÓSTICO 25
3.7 BUSQUE FERRAMENTAS OU UTILIZAÇÃO DE BANCO DE DADOS CENTRALIZADO 25
3.8 CONSTRUÇÃO DO PROGRAMA DE GOVERNANÇA 25
3.9 DOCUMENTOS JURÍDICOS 26
3.10 TREINAMENTO PARA CONSCIENTIZAÇÃO 26
3.11 CHECKLIST 27
4. COMO SE ADEQUAR **30**
4.1 RELAÇÕES DE TRABALHO 31
4.1.1 DADOS PESSOAIS TRATADOS NOS PROCESSOS DA RELAÇÃO DE TRABALHO 32
4.1.2 TRANSMISSÃO DE DADOS PESSOAIS DECORRENTES DA RELAÇÃO DE TRABALHO A TERCEIROS 38
4.2. RELAÇÕES COMERCIAIS 39
4.2.1 DADOS DE CLIENTES 39
4.2.2 ENVIO DE INFORMATIVOS E MEIOS DE COMUNICAÇÃO 40
4.2.3 COMO REGULAMENTAR AS RELAÇÕES COM PARCEIROS 43
4.3 RELAÇÕES ADMINISTRATIVAS 47
4.3.1 COMO ADMINISTRAR RELAÇÕES COM TERCEIROS 47
4.3.2 COMO TRATAR DADOS PESSOAIS DE REPRESENTANTES LEGAIS/PROCURADORES 49
5. A LGPD PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE **51**
5.1. A QUEM SE APLICA? 52
5.2. DAS OBRIGAÇÕES 54
5.3. DA NOMEAÇÃO DO ENCARREGADO 54
5.4. DA SEGURANÇA E BOAS PRÁTICAS 54
5.5. PRAZOS ESPECÍFICOS 55
6. PERGUNTAS FREQUENTES (FAQ) **56**

LEGISLAÇÃO

LEGISLAÇÃO

1.1 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

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 Pessoais (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).

Vale mencionar que a LGPD não surge com o objetivo de coibir e vedar a utilização de Dados Pessoais pelas empresas, mas visa estabelecer premissas e parâmetros mínimos que devem ser observados nesta coleta e em qualquer tratamento realizado. Assim, também de forma harmônica com o respeito à privacidade do indivíduo, a Lei também determina, em seu artigo 2º, como fundamentos elementares e necessários da disciplina de proteção de *Dados o desenvolvimento econômico e tecnológico*, bem como a *inovação, livre iniciativa e livre concorrência*, aspectos essenciais para o fomento sustentável da tecnologia e dos negócios, tendo como pressuposto a segurança jurídica como lógica garantidora da lei.

No dia a dia empresarial, diversos Dados Pessoais são tratados e registrados para, por exemplo, cadastro de clientes, envio de comunicados, convites, promoções, elaboração de contratos em razão dos serviços avençados, além de uma série de outras atividades. Logo, Dados Pessoais como CPF, RG, e-mail e até mesmo cargo precisam de atenção no tratamento.

Assim, a LGPD surge no Brasil em um contexto de harmonização e atualização de conceitos, a fim não só de gerar maior segurança jurídica e instituir uma exigência legal no âmbito da privacidade e proteção de Dados, mas também para atrair investimentos do exterior e instaurar um diferencial competitivo cujos países ao redor do mundo requerem na atual conjuntura.

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, todo segmento empresarial que venha a realizar qualquer tipo de tratamento de Dados Pessoais, por meio físico ou digital. 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?

Traremos a definição de "Dado Pessoal" de maneira mais robusta no Glossário Exemplificativo (Capítulo 2 deste Guia), mas antes de adentrarmos ao tratamento de um Dado, vale pincelarmos, de forma breve, o que é um Dado Pessoal à luz da LGPD. Constitui, dessa maneira, *qualquer informação relacionada à pessoa natural que possa ser identificada ou identificável, ou seja, qualquer Dado que possa permitir a identificação de uma pessoa física de forma individualizada*.

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 daquelas atividades contempladas na Lei, de forma que, por "tratamento" podemos entender como 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.

Exemplo: quando a empresa **acessa** uma planilha que contenha e-mail e endereço de clientes que os identifiquem/individualizem de maneira singular, ou, ainda, **armazena** dados telefônicos para envio de informações comerciais, já há o tratamento de Dados Pessoais.

QUANDO POSSO TRATAR UM DADO?

A LGPD não é impeditiva quanto ao tratamento de Dados Pessoais, mas dentre um dos aspectos a serem observados para legitimar este tratamento tem-se a escolha de uma "Base legal", a denominada *hipótese autorizadora* pela LGPD.

Lembre-se que é responsabilidade do Controlador a escolha da base legal aplicável ao tratamento.

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 empresariais, sem prejuízo da utilização das demais, quando aplicável e sempre em análise ao caso concreto:

• **(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 da LGPD), **impedindo, por exemplo, a utilização das Bases Legais do legítimo interesse, da execução de contrato e da proteção ao crédito para o tratamento de Dados sensíveis**. Além disso, podemos tratar um Dado Pessoal sensível, por exemplo, nas seguintes hipóteses:

- Na garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos; e
- No 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 ao titular, não sendo possível a utilização para finalidades genéricas ou tratamento posterior de forma incompatível com as finalidades originais. Ou seja, deve-se ter um objetivo específico para o tratamento daquele Dado, explicando ao titular este motivo. 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 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: um cliente preencheu formulário para realização de um webinar X. A finalidade informada ao titular para o tratamento dos Dados por ele fornecidos, foi, portanto, garantir sua participação no evento. A empresa, assim, não pode utilizar esses Dados para finalidades diversas, como encaminhá-los para a equipe de comunicação realizar uma abordagem oferecendo demais serviços. Assim:

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

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 integridade 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 de sua empresa e indique quais Dados Pessoais são tratados, as bases legais, 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, principalmente levando em consideração o público-alvo ao qual aquele aviso se destina;
- Não compartilhe os Dados Pessoais com terceiros de forma oculta, o titular deve estar sempre ciente de qualquer compartilhamento de suas informações e das finalidades relacionadas, já que o compartilhamento é considerado também uma atividade de *tratamento* de Dados.

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 (como elaboração de contratos com parceiros envolvidos) 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 e a quem de fato precisa.

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 com 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. A 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 encarregado 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**, que entraram em vigor **a partir de 1º de agosto de 2021**, podem ser aplicadas simplesmente em razão do descumprimento de qualquer uma das disposições legais contidas na LGPD e, por este motivo, a adequação inicial – mas perene – das empresas ao disposto na Lei constitui etapa relevante e fundamental diante deste cenário.

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.

Importante ressaltar que embora as sanções administrativas tenham começado a valer apenas em 1º de agosto de 2021, com a LGPD em vigor desde 18 de setembro de 2020, ações judiciais e indenizações, inclusive por órgãos de defesa do consumidor, já vêm sendo, respectivamente, ajuizadas e aplicadas em massa com amparo nas disposições contempladas na Lei, exigindo-se, dessa forma, que os Agentes de Tratamento estejam em um processo de conformidade à legislação e seus princípios norteadores.

Atenção: Em 28 de outubro de 2021, houve a aprovação da Resolução CD/ANPD nº 1 , que institui Regulamento de Fiscalização e de Aplicação de Sanções Administrativas. De modo a conferir segurança jurídica aos administrados, a ANPD iniciou sua atuação sancionadora após a aprovação do Regulamento. Sua atuação, no entanto, pode se dar com relação a fatos ocorridos após 1º de agosto de 2021 ou para delitos de natureza continuada iniciados antes de tal data.

O texto do Regulamento, que se aplica aos titulares de Dados, Agentes de Tratamento e demais interessados no tratamento de Dados Pessoais (conforme Art. 13º), estabelece as etapas do processo administrativo sancionador e os direitos dos administrados, iniciando a atuação sancionadora da entidade. Ademais, o texto define os deveres dos agentes regulados (Art. 5º):

- O fornecimento de cópia de documentos físicos e digitais, informações e Dados relevantes para a avaliação das atividades de tratamento de Dados Pessoais nos termos estabelecidos pela ANPD.
- Permissão de acesso a equipamentos, instalações, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, documentos e informações de natureza técnica, operacional e outras pertinentes para a avaliação do tratamento de Dados e que estejam em seu poder ou de terceiros.
- Dar conhecimento a ANPD dos sistemas de informação utilizados para tratamento de Dados e informações, assim como sua rastreabilidade, atualização e substituição, disponibilizando ainda os Dados e informações daí oriundos.
- Submeter-se a auditorias.
- Manter armazenamento de documentos, informações e Dados pelos prazos definidos em legislação e regulamentação específica ou durante todo o prazo de tramitação de processos administrativos.
- Disponibilizar, quando solicitado, representante para suporte a ANPD.

O não cumprimento dos deveres listados caracterizará obstrução da atividade de fiscalização, sujeitando o infrator às medidas repressivas cabíveis, sem prejuízo da adoção de outras medidas necessárias para conclusão da atividade de fiscalização (Art. 16º).

Ainda quanto à atuação da ANPD, esta se dará conforme uma abordagem responsiva, ou seja, de maneira gradual, baseada no comportamento do regulado e baseada em um plano de monitoramento do setor que permita a priorização de temas segundo seu risco, gravidade, atualidade e relevância. Assim, a ANPD estabelece que a fiscalização compreenderá às atividades de monitoramento, orientação e atuação preventiva.

Por sua vez, 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.

Vale mencionar também que **norma específica** contendo as metodologias que orientarão o **cálculo do valor-base das sanções** de multa ainda será objeto de consulta pública pela ANPD.

A **comunicação à ANPD** quanto a eventuais infrações relacionadas com a LGPD poderá ser realizada por canal apropriado, já existente no site da Autoridade. As instruções completas podem ser consultadas por meio do link: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/reclamacao-do-titular-contra-controlador-de-dados

NOTIFICAÇÕES DE INCIDENTES – QUANDO SÃO OBRIGATÓRIAS

O Controlador, quando exigido por lei, 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, observados os segredos comercial e industrial;

(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.

O que é um risco ou dano relevante?

Critérios mais objetivos serão objeto de futura regulamentação pela ANPD. A Autoridade, no entanto, já dispôs acerca do tema, de maneira que se pode extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade.

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;

- Definir e classificar, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais/equipe responsável e a depender do contexto, quais Dados Pessoais acarretariam risco ou dano relevante aos titulares para que se verifique a necessidade de comunicação ou não do incidente à ANPD e aos titulares. Perguntas a serem utilizadas internamente para guiar esta avaliação foram disponibilizadas pela ANPD em seu website.

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

- 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.

1.3. LGPD E EMPRESAS

Diversos Dados Pessoais são tratados diariamente e registrados para o envio de comunicados, promoções, convites, informativos, cobranças, registros de clientes, bem como outras atividades, sendo, portanto, fundamental que as empresas tenham cuidado com a coleta, tratamento e qualquer outra atividade que envolva Dados Pessoais, bem como observem todos aqueles (como colaboradores/parceiros) que de alguma forma se relacionam no exercício de suas atividades.

É de conhecimento, portanto, que a LGPD, como regra geral e ressalvadas as hipóteses previstas em lei, se aplica a todas as empresas, de qualquer porte e segmento, desde que (i) a operação de tratamento seja realizada no território nacional; (ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou (iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Contudo, a LGPD, em seu artigo 55-J, XVIII, prevê uma especial atenção às microempresas, empresas de pequeno porte, aquelas que se autodeclarem *startups* e empresas de inovação, bem como a pessoas físicas que tratem Dados Pessoais com fins econômicos, estabelecendo como competência da ANPD a edição de normas, orientações sobre o assunto e procedimentos simplificados e diferenciados, inclusive quanto aos prazos. Tal entendimento foi consolidado na Resolução CD/ANPD nº 2 , que versa sobre tratamento jurídico específico aos Agentes de Tratamento de pequeno porte, conforme capítulo 5 deste Guia Orientativo.

Diante da nova legislação, no tocante às empresas, **o olhar deve estar voltado a 3 (três) relações principais, quais sejam, de (i) trabalho** – ex: colaboradores e empregados; **(ii) comerciais** - ex: clientes e parceiros de negócio; e **(iii) administrativas**, terceiros de maneira geral - ex: prestadores de serviços.

Assim, para a relação de **Trabalho**, os Dados Pessoais, desde que observados os princípios, bases legais e demais disposições legais, 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 fins de transparência, recomenda-se a elaboração de um Aviso de Privacidade Interno (destinado ao colaborador).

Quanto à relação **Comercial** com clientes (principalmente no âmbito das empresas B2C), aos titulares envolvidos deve-se dar total transparência a respeito de, por exemplo, quais Dados Pessoais são coletados e tratados, bem como as finalidades atreladas, duração do tratamento, armazenamento, dentre outros. Em relação aos parceiros de negócio e aos clientes B2B, merece destaque os contratos firmados entre as partes que definirão as responsabilidades inerentes a cada uma enquanto Agentes de Tratamento daquela relação, estabelecendo os critérios e padrões mínimos para condução do tratamento. Para a transparência aos clientes (pessoas físicas), recomenda-se a elaboração de um Aviso de Privacidade Externo.

Por fim, na relação **Administrativa**, com terceiros de maneira geral, no caso em que houver o compartilhamento e tratamento de Dados Pessoais entre as Partes, deve-se também estabelecer contratos com cláusulas para definição das responsabilidades entre os agentes. Para a transparência, recomenda-se também a elaboração de um Aviso de Privacidade Externo.

Em todas as relações, cumpre destacar a importância em se instituir um Programa de Governança dentro das empresas, de maneira a criar políticas e procedimentos que regulem os aspectos de privacidade e proteção de Dados Pessoais dentro da organização.

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 de dados e utilizar conscientemente as informações dos Colaboradores, Clientes/Parceiros e Terceiros de modo a fornecer-lhes diretrizes de boas práticas e máxima transparência.

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.

GLOSSÁRIO EXEMPLIFICATIVO

GLOSSÁRIO EXEMPLIFICATIVO

Agentes de Tratamento, nos termos do disposto na LGPD: O Controlador e o Operador.

Atenção: A ANPD publicou em maio de 2021 o 1º documento orientador intitulado "Guia Orientativo para Definições dos **Agentes de Tratamento** de Dados Pessoais e do **Encarregado**", que busca estabelecer diretrizes não-vinculantes aos Agentes de Tratamento e explicar quem pode exercer a função do Controlador, do Operador e do Encarregado.

Através do Guia e, apesar de não haver menção expressa a tais definições na LGPD, a ANPD traz, inspirada em outras legislações do cenário europeu, as seguintes figuras:

- **Controladoria Conjunta** – quando há participação conjunta por dois ou mais Controladores na determinação das finalidades e os meios de tratamento. As finalidades, assim, podem ocorrer a partir de decisões comuns (há uma intenção comum sobre as finalidades) ou convergentes (decisões distintas sendo tomadas, porém elas se complementam de tal forma que o tratamento não seria possível sem a participação de ambos os Controladores);– e **Singular** – quando os objetivos e as finalidades não forem comuns, convergentes ou complementares, ambos os Controladores serão Controladores singulares em relação ao tratamento de Dados.

- **Suboperador** - aquele contratado pelo Operador para auxiliá-lo no tratamento dos Dados Pessoais em nome do Controlador.

Lembre-se que a definição do Agente de Tratamento estará vinculada a cada atividade exercida em específico. Em outras palavras, por ser um conceito dinâmico, em uma mesma relação contratual, cada parte poderá desempenhar em cada momento um papel diferente de Agente de Tratamento, de acordo com a atividade exercida.

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, informada e inequívoca, de maneira que o titular dos Dados concorda mediante ato positivo que seus Dados Pessoais sejam tratados para finalidade determinada. Devendo ser:

(I) Livre - deve ser conferido o efetivo poder de escolha ao titular de quais Dados fornecer e quais não fornecer, além de ser capaz de revogar o seu consentimento a qualquer momento;

(II) Informado – previamente à realização do tratamento, devem ser fornecidas informações claras, precisas e facilmente acessíveis aos titulares dos Dados, como as finalidades para as quais o tratamento de Dados se destina e a duração do tratamento; e

(III) Inequívoco - requer a demonstrabilidade de que o titular de fato 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 aquele Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento. Os dados anonimizados não serão considerados Dados Pessoais para os fins da LGPD salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Exemplo: Anonimização de Dados Pessoais de clientes fidelizados 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 – ainda assim, alguns Dados relativos às pessoas jurídicas, por sua natureza, podem tornar uma pessoa física identificável, a exemplo do Microempreendedor individual (MEI), cuja razão social é constituída pelo seu próprio nome e número do seu CPF, individualizando-o, portanto. Dados Pessoais de representantes legais e procuradores, por sua vez, se passíveis de identificá-los, também devem ser tratados como Dados Pessoais.

Dado Pessoal Sensível: É a informação relacionada à 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 pelo Tratamento de Dados Pessoais (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 Encarregado, 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.

Como boa prática, considera-se importante que o Encarregado tenha liberdade na realização de suas atribuições.

Apesar da obrigação de nomeação do Encarregado ser, nos termos da LGPD, do Controlador (com exceção do Poder Público, que, nos termos do art. 23, III e 39 da LGPD, deverá instituir Encarregado quando realizar quaisquer operações de tratamento de Dados Pessoais), 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 e/ou normativas futuras nesse sentido, sugere-se a indicação de um Encarregado para qualquer organização que trate Dados Pessoais.

Vale ressaltar que, conforme Resolução CD/ANPD nº 2, os Agentes de Tratamento de pequeno porte não são obrigados a indicar o Encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD, devendo, no entanto, nestes casos, disponibilizar um canal de comunicação para que seja possível o atendimento de requisições pelo Titular.

Por fim, cumpre pontuar que em abril de 2022, houve início das reuniões técnicas relativas à tomada de subsídio para elaboração de minuta da norma sobre o Encarregado pelo tratamento de dados pessoais.

Incidente de segurança envolvendo Dados Pessoais: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos Dados Pessoais.

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.

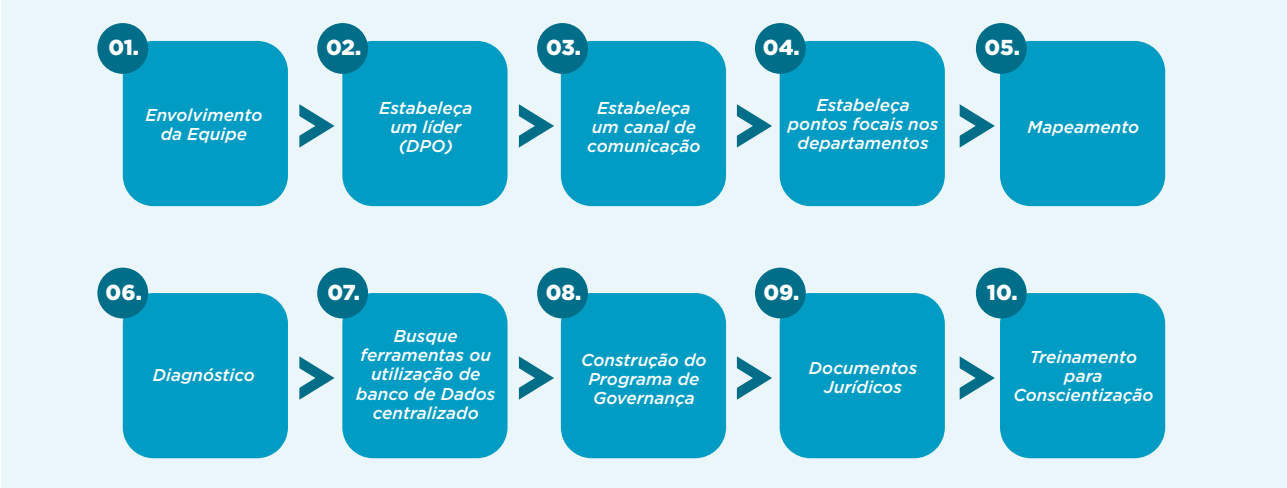
PRINCIPAIS PASSOS PARA O INÍCIO DO PROCESSO DE ADEQUAÇÃO/ CONFORMIDADE

PRINCIPAIS PASSOS PARA INÍCIO DO PROCESSO DE ADEQUAÇÃO

Primeiramente, é importante que as organizações ponderem e levem em consideração em seus respectivos processos de adequações, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de Dados que lhes competem. Nesta toada, é imprescindível que haja a observância também à toda legislação setorial e regulatória aplicável, a exemplo de empresas do ramo de saúde, bancário e de aviação.

Privacy by Design: o conceito desenvolvido por Ann Cavoukian encontra previsão legal na LGPD de forma expressa em seu artigo 46, §2 e constitui um ótimo norteador não só para as ações e projetos, mas inclusive para ideias embrionárias que se tenha em qualquer atividade envolvendo o tratamento de Dados Pessoais dentro da empresa. O objetivo é conferir uma perspectiva de privacidade desde a concepção. Ou seja, significa que todas as etapas do processo de desenvolvimento de um produto ou serviço que uma empresa oferece devem ter a privacidade e os demais aspectos inerentes a ela "embutidos" e "enraizados" desde o início de qualquer etapa do processo.

Passos para o início do Processo de Adequação:



3.1. ENVOLVIMENTO DA EQUIPE

Buscar o envolvimento da alta liderança, a exemplo de membros da Diretoria, Conselho de Administração – se existente , times jurídicos, comercial, de Tecnologia da Informação, 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 PELO TRATAMENTO DE DADOS PESSOAIS - DPO)

O Encarregado pelo tratamento dos Dados Pessoais será o porta-voz da empresa 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 para todos os Agentes de Tratamento, com exceção definida aos Agentes de Tratamento de pequeno porte conforme Resolução CD/ANPD nº 2, e do Poder Público, que, nos termos do art. 23, III e 39 da LGPD,deverá instituir Encarregado quando realizar quaisquer operações de tratamento de Dados Pessoais, . De todo modo, a figura do Encarregado é recomendável para qualquer organização.

Como já mencionado, em abril de 2022, houve início das reuniões técnicas relativas à tomada de subsídio para elaboração de minuta da norma sobre o Encarregado pelo tratamento de dados pessoais. Assim, atente-se a atualizações quanto a este tema.

QUEM PODE SER UM ENCARREGADO/DPO?

O Encarregado pode ser qualquer pessoa, inclusive jurídica ou até mesmo pessoa terceirizada alheia à empresa. 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 da empresa. Contudo, é recomendável evitar que estas outras funções gerem conflitos de interesse com o papel esperado do Encarregado. Exemplo: este conflito pode surgir, eventualmente, da cumulação de cargos que realizam e/ou supervisionam muitas atividades de tratamento de Dados, as quais precisam ser auditadas pelo Encarregado de forma imparcial.

QUAL QUALIFICAÇÃO O ENCARREGADO DEVE TER?

No que diz respeito às suas qualificações profissionais, estas devem ser definidas mediante um juízo de valor realizado pelo Controlador que o indica, considerando conhecimentos de proteção de dados e segurança da informação em nível que atenda às necessidades da operação da organização.

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

- Lei Geral de Proteção de Dados Pessoais e aspectos de Segurança da Informação;
- Regulamentações pertinentes às atividades da empresa 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 pela empresa; e
- As necessidades específicas e desafios da empresa 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 in- formação, além de entender as operações de tratamento de Dados Pessoais realizadas pela empresa; 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, mas o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado", da ANPD, já estabelece alguns parâmetros, como a indicação do Encarregado por um ato formal. Nesta linha e inclusive 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) 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 da empresa.

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 da empresa.

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 da 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.

Importante: Cabe lembrar que os direitos dos titulares não são absolutos, ou seja, em algumas situações, a solicitação do titular pode não ser atendida (parcial ou totalmente), a exemplo do caso em que a empresa não seja o Controlador daqueles Dados Pessoais. Nesta situação, contudo, terá a empresa a obrigação de comunicar, por exemplo, que não é o Agente de Tratamento, indicando, se possível, o respectivo agente.

3.4. ESTABELEÇA PONTOS FOCAIS NOS DEPARTAMENTOS

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 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 atividades de tratamento (ROPA), em linha com o definido pelo artigo 37 da LGPD, constitui elementos estruturantes de suma importância, sendo obrigatória a sua conservação, inclusive, para fins de controle interno, auditoria e fiscalização da ANPD. Entretanto, como discutido em detalhes na seção 5 deste Guia, a Resolução CD/ANPD nº 2 prevê condições específicas aos Agentes de Tratamento de pequeno porte para o registro de atividades de tratamento.

Assim, saiba, minimamente:

- 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 a empresa, 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 e de crianças;
- 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

Busque um 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.

Lembre-se que caso se opte pela contratação de um parceiro, é de suma importância que se firme um contrato apto a definir as responsabilidades das partes enquanto Agentes de Tratamento daquela relação.

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 criticidade 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, quando aplicável;
- 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 e proteção de dados seja na relação com o titular dos Dados seja em contratos com terceiros. Políticas e Procedimentos relativos ao Programa de Governança interno devem ser observados por todos da organização e por aqueles com quem ela de alguma forma se relaciona e que esteja envolvida no tratamento e/ou compartilhamento de Dados Pessoais da instituição.

- **Adeque contratos com terceiros** em que há o compartilhamento e tratamento de Dados Pessoais, inserindo e definindo as responsabilidades de cada Agente de Tratamento. Importante mencionar que mesmo que inicialmente não se verifique tratamento de dados na relação com o parceiro, é recomendado que se inclua cláusulas relativas à privacidade e proteção de dados, mesmo que de forma mais geral.

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** da empresa, quando existente, tendo em vista a aplicabilidade das disposições ali dispostas aos colaboradores. Para as empresas 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 da empresa e por aqueles com quem ela 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, clientes pessoa jurídica) 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 terceiros no geral (incluindo, em alguns casos, os próprios clientes pessoa física) e visitantes da página; (iii) Política Geral de Privacidade e Proteção de Dados Pessoais; (iv) Política de Compartilhamento de Dados Pessoais e (v) Plano de Resposta a Incidentes. A elaboração de mais ou menos políticas e procedimentos deve considerar os aspectos fáticos de cada empresa, como porte, volume e natureza dos dados e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

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. Vale ressaltar que este é um aspecto importante inclusive para demonstrar a adoção pelo Agente de Tratamento de medidas de cumprimento ao disposto na LGPD.

3.11. CHECKLIST

Aqui sugerimos um *checklist* sobre as ações iniciais para adequação à LGPD, seguindo os passos descritos acima. Reiteramos que este Guia Orientativo indica, de forma exemplificativa, os principais passos para o início da jornada de conformidade das atividades de tratamento de Dados pela empresa, e que, portanto, não tem a finalidade de esgotar a análise da matéria, considerando-se, inclusive, que o processo de adequação é contínuo e perene. Ainda, este *checklist* e demais medidas a serem observadas deverão ser calibrados de acordo com cada empresa e suas respectivas prioridades.

ENVOLVIMENTO DA EQUIPE

- ☐ Comunicado/Se aplicável, cronograma de trabalhado definido com o setor jurídico
- ☐ Comunicado/Se aplicável, cronograma de trabalhado definido com o setor de TI
- ☐ Comunicado/Se aplicável, cronograma de trabalhado definido com o setor de RH
- ☐ Comunicado/Se aplicável, cronograma de trabalhado definido com o setor financeiro
- ☐ Comunicado/Se aplicável, cronograma de trabalhado definido com todos os funcionários
- ☐ Comunicado/Se aplicável, cronograma de trabalhado definido com executivos e sócios
- ☐ Comunicado/Se aplicável, cronograma de trabalhado definido com os diretores
- ☐ Comunicado/Se aplicável, cronograma de trabalhado definido com o Conselho de Administração
- ☐ Outros: _____

ESTABELEÇA UM LÍDER (ENCARREGADO - DPO)

- ☐ Identificada e comunicada uma pessoa para ser o/a Encarregado (a)
- ☐ Esta pessoa possui os conhecimentos mínimos necessários
- ☐ Esta pessoa possui as habilidades mínimas necessárias
- ☐ Termo de confidencialidade/Termo de posse assinado
- ☐ Identidade e informações de contato divulgadas publicamente e disponíveis no website
- ☐ Estabelecimento de um cronograma de trabalho

ESTABELEÇA UM CANAL DE COMUNICAÇÃO

- ☐ Contato com Encarregado disponível no website e outros meios
- ☐ Formulário no website disponível ao titular para atendimento de solicitação

☐ Definição de procedimentos/scripts para atendimento dos direitos dos titulares e respectiva validação da identidade deste

☐ Equipe organizada e informada sobre procedimentos e como atender

ESTABELEÇA PONTOS FOCAIS NOS DEPARTAMENTOS

☐ Estabelecidos e treinados os pontos focais para auxiliarem o Encarregado

☐ Equipe organizada e informada sobre procedimentos e como reportar ao Encarregado

REÚNA INFORMAÇÕES SOBRE OS DADOS COLETADOS - MAPEAMENTO

☐ Reuniões com cada área para mapear os fluxos internos que envolvem o tratamento de Dados Pessoais

☐ Registro das atividades de tratamento em documento específico (ROPA)

☐ Criação de processo de revisão do ROPA

ANALISE SE OS DADOS ESTÃO SENDO TRATADOS CONFORME A LGPD – DIAGNÓSTICO

☐ Divisão dos processos de cada departamento e definição da categoria de Dados tratados

☐ Verificado se os Dados existentes estão adequados às Bases Legais

☐ Analisado se o compartilhamento dos Dados está seguro e descrito nos contratos

☐ Identificados os gaps

☐ Formulada uma matriz de risco

☐ Instaurado plano de ação, em razão dos gaps identificados

BUSQUE FERRAMENTAS OU UTILIZAÇÃO DE BANCO DE DADOS CENTRALIZADO

☐ Revisadas as ferramentas e sistemas atualmente utilizados na empresa

CONSTRUÇÃO DO PROGRAMA DE GOVERNANÇA

☐ Estabelecimento de políticas e salvaguardas adequadas

☐ Assegurada a transparência e estabelecimento da relação com o titular

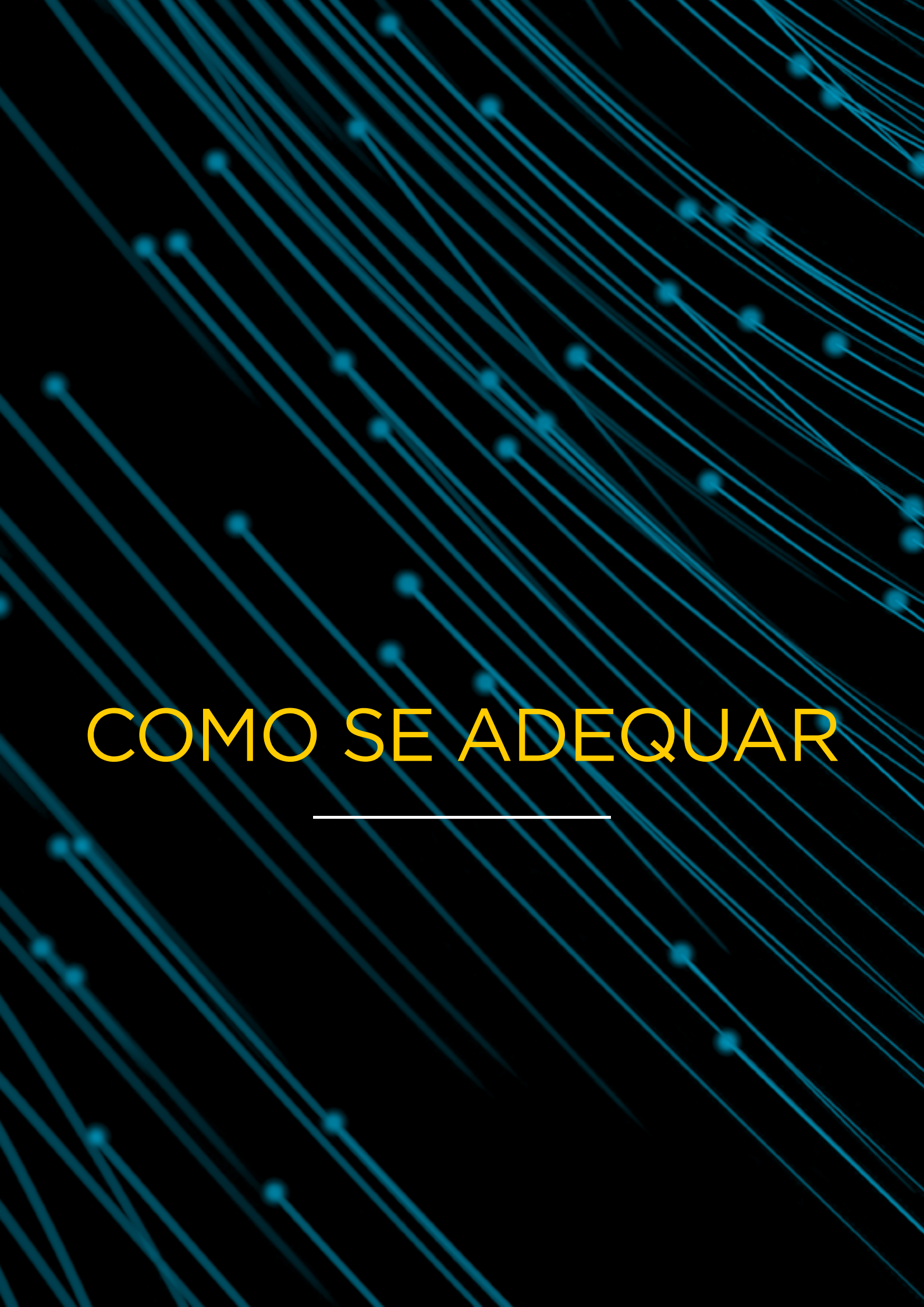
- ☐ Aplicados mecanismos de supervisão internos e externos
- ☐ Planos de resposta a incidentes e remediação criados
- ☐ Programa de Governança devidamente criado

DOCUMENTOS JURÍDICOS

- ☐ Revisados todos os documentos jurídicos pertinentes
- ☐ Adequação de contratos com terceiros
- ☐ Inclusão de disposição sobre privacidade e proteção de Dados no Código de Ética e Conduta da empresa
- ☐ Revisão ou instituição de uma Política Geral de Privacidade e Proteção de Dados Pessoais
- ☐ Revisão ou instituição de demais políticas, procedimentos e avisos

TREINAMENTO PARA CONSCIENTIZAÇÃO

- ☐ Realização de treinamentos e reuniões de alinhamento
- ☐ Apresentação das novas políticas e diretrizes de proteção de Dados Pessoais
- ☐ Disseminação da cultura organizacional


COMO SE ADEQUAR

COMO SE ADEQUAR

Passemos agora para um passo a passo mais específico em relação ao tratamento de Dados Pessoais pela empresa quando do exercício de atividades nas relações **(i) de trabalho** (ex: colaboradores e empregados); **(ii) comerciais** (ex: clientes e parceiros de negócio) e **(iii) administrativas** (ex: 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** ou qualquer outro meio que demonstre transparência ao candidato.

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 instituição, 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. 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 eventos 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 da empresa, 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 A EMPRESA, PERMITINDO SUA UTILIZAÇÃO E ARMAZENAMENTO?

A obtenção do consentimento só será necessária se não for possível que a empresa 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) da empresa também poderá ser utilizada. Vale ressaltar que a escolha da base legal aplicável à atividade de tratamento ficará à critério do Controlador, nos termos da lei.

Ao ser admitido no processo seletivo e ao dar início à etapa de contratação do candidato, é importante que a empresa 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 de informações 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 (ou até mesmo a garantia da prevenção à fraude e segurança do titular, no caso de biometria), e não o consentimento.

Ainda, importante ressaltar que, caso seja necessário o **compartilhamento desses Dados Pessoais com outras empresas recrutadoras**, por exemplo, se a empresa 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 ou outro meio de transparência 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, 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 a empresa, 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, onde se aplique, 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 pela instituição, 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.

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 na empresa, 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 da empresa), 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*

No entanto, sem prejuízo do disposto acima, é possível também que as responsabilidades do empregado e do empregador quanto ao manuseio dos dados pessoais da empresa estejam dispostas expressamente no Contrato de Trabalho.

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.

Válido ressaltar que, como boa prática e de forma a mitigar eventuais riscos, não há prejuízo de inserção também de dispositivo atinente à privacidade e proteção de Dados no contrato de trabalho do empregado – sendo esta, inclusive, prática adotada pela maioria das empresas -, incluindo mas não se limitando à remissão das respectivas políticas impostas pela empresa e que devem ser observadas pelo empregado, vinculando-o em relação ao seu cumprimento; bem como inserção de remissão ao Aviso de Privacidade Interno de maneira a reforçar que empregador cumpre com seu dever de transparência em relação ao empregado enquanto titular de Dados, além de aspectos inerentes ao cumprimento da legislação vigente sobre privacidade e proteção de dados pessoais.

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. As empresas 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, caso não haja finalidade que autorize a continuidade do tratamento dos Dados, 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 incidentes.

Porém, é válido pontuar que, de maneira geral, documentos previdenciários e trabalhistas (contrato de trabalho, rescisão, aviso prévio, dentre outros), podem permanecer armazenados na instituição 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 na empresa 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 informa-lo sobre o tratamento e transferência/compartilhamento de seus Dados Pessoais, para quais empresas – se aplicável – e para qual finalidade e, se necessário e aplicável, colete o devido consentimento para que os Dados sejam transferidos a terceiros.

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

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, a empresa deverá 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) ou em qualquer outra Base Legal aplicável.

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 de Tratamento 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 ao tratamento de Dados Pessoais de dependentes menores de 12 anos incompletos, o consentimento deve ser coletado, obrigatoriamente, nos termos da lei, de 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.

4.2. RELAÇÕES COMERCIAIS

4.2.1. DADOS DE CLIENTES

Para que se defina a estratégia e os aspectos de privacidade e proteção de Dados Pessoais a serem aplicados, é importante que, como primeiro passo, a empresa verifique se há um envolvimento direto com o titular dos Dados, pessoa física, como ocorre no âmbito das empresas B2C; ou se o cliente na realidade será uma pessoa jurídica, a exemplo do que acontece nas relações de organizações B2B.

Aos titulares envolvidos deve-se dar total transparência a respeito de quais Dados Pessoais são coletados e tratados, a exemplo da disponibilização de tais informações através do Aviso de Privacidade Externo divulgado no website. Já em relação aos parceiros de negócio e às organizações B2B, merecem destaque os contratos firmados entre as partes de modo a definir as responsabilidades inerentes a cada uma enquanto Agentes de Tratamento daquela relação, estabelecendo os critérios e padrões mínimos para condução do tratamento.

QUAIS DADOS DEVO SOLICITAR PARA CADASTRO?

Lembre-se sempre: **caso seus clientes sejam pessoas físicas**, eles são proprietários (titulares) de seus próprios Dados Pessoais. Por exemplo, os Dados Pessoais, como nome, endereço residencial, documentos de identificação e telefone devem ser protegidos.

Novamente, a LGPD não prevê a descrição de quais Dados Pessoais podem ser solicitados para o cadastro de um cliente, por exemplo, de maneira que podem variar a depender das características e necessidades requeridas para a atividade-fim. Desta forma, além de verificar a Base Legal adequada, as finalidades e informações acerca deste tratamento devem estar disponíveis de maneira clara ao titular, assim como deve- se obter apenas o mínimo necessário e observar todos os demais princípios e disposições da LGPD.

Exemplo: sua empresa possui um cadastro de clientes pessoa física para fornecer descontos. Dados como endereços ou até mesmo data de nascimento não são necessários para este fim. Avalie quais Dados são realmente necessários, dê a devida transparência ao cliente quanto aos Dados tratados naquela atividade e limite o uso de seus Dados para somente aquela finalidade da qual ele foi informado, sem que haja o desvio para outra atividade, como o envio de e-mails com promoções, por exemplo.

É importante também, informar ao titular, através do **Aviso de Privacidade** disponibilizado no website (verifique o Capítulo 1, na página 10).

Caso seus clientes sejam pessoas jurídicas, e a sua empresa não tenha contato direto com o titular dos Dados, é importante ao menos garantir contratualmente que o cliente, quando na qualidade de Controlador dos Dados, foi transparente com o titular em relação à utilização de seus Dados e definiu Base Legal que autoriza o respectivo tratamento, inclusive no tocante a eventual compartilhamento com terceiro.

4.2.2. ENVIO DE INFORMATIVOS E MEIOS DE COMUNICAÇÃO

PARA O ENVIO DE INFORMATIVOS E MEIOS DE COMUNICAÇÃO É NECESSÁRIO O CONSENTIMENTO DO TITULAR?

Como visto anteriormente, a LGPD preza por uma relação transparente entre as partes, no caso, as empresas, empregados, clientes, parceiros de negócio e terceiros prestadores de serviços, bem como outros usuários. O princípio desta relação, portanto, deve estar fundamentado em Base Legal que autorize o tratamento dos Dados Pessoais do titular e, para realizar esse enquadramento, lembre-se de se ter em mente a finalidade para qual o Dado Pessoal será tratado.

De maneira geral, para **ações de comunicação**, como envios de e-mail marketing e SMS, envio de convite a eventos, notícias, dentre outros, a **Base Legal do consentimento** será a mais adequada. Sendo este o cenário, a autorização deve ser concedida pelo titular de forma livre, inequívoca e informada (no caso de dúvidas, consulte novamente o glossário exemplificativo).

Um ponto importante é que a Lei exige que o consentimento seja solicitado para fins específicos pelo Controlador,

além de indicar expressamente que as "autorizações genéricas para o tratamento de Dados Pessoais serão nulas", ou seja, sem efeito, desconsideradas. Os Dados requisitados devem ser utilizados para cumprir somente a finalidade inicialmente disposta e nenhuma outra ação não informada ao titular.

Exemplo: se solicitado consentimento para o tratamento de Dados Pessoais para a finalidade de realização de um evento da empresa, esses Dados não poderão ser utilizados para envio de e-mail marketing (outra finalidade).

Esta permissão, que deverá ser fornecida por escrito ou por outro meio que permita a demonstração da manifestação de vontade do titular, pode ser solicitada através de processos de ***opt-in*** – processo de permissão simples, no qual ao se cadastrar em formulário de cadastro para receber um *newsletter*, por exemplo, o titular concede a permissão para próximos envios – ou de **dupla confirmação *(double opt-in)*** – um *opt-in* reforçado, no qual, além do titular demonstrar seu interesse em receber comunicados, a empresa deve enviar um e-mail com um link de confirmação de assinatura.

É preciso ressaltar, contudo, que o procedimento de *opt-in* nada mais é do que uma permissão que o titular concede para autorizar um determinado tratamento de dados. Ou seja, não deve ser confundido ou compreendido como sinônimo da Base legal do Consentimento. Quando oferecida a opção de *opt-in* ao titular para qualquer atividade de tratamento, é necessário identificar em qual das hipóteses o *opt-in* está sendo adotado, e em qual cenário este procedimento estaria inserido para fins de coleta do consentimento previsto na LGPD. Isso porque, como já visto, esta Base Legal carece de requisitos específicos para ser considerada válida.

Caso o usuário não tenha interesse em receber comunicados e não dê a permissão (caso a Base Legal seja o consentimento), nenhum comunicado poderá ser enviado, respeitando sua livre decisão. Lembre-se que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, sendo de extrema importância que se tenha um controle e gestão dessas autorizações para que, caso solicitado, haja a exclusão desses Dados Pessoais de forma facilitada (***opt-out*** nesta hipótese, o *opt-out* refletirá a revogação do consentimento fornecido, caso seja essa a Base Legal adotada). Neste caso, deve a empresa fazer a gestão adequada de tais consentimentos para se assegurar de que não sejam direcionados comunicados aos titulares em listas para as quais ele tenha dado *opt-out*, sob pena de a instituição tratar dados pessoais sem possuir uma Base Legal adequada para o tratamento.

Vale mencionar que quando a Base Legal escolhida for o Legítimo Interesse, o *opt-out* corresponde a uma boa prática a ser implementada por parte da empresa enquanto Controladora, e servirá para reforçar a expectativa do titular para o tratamento de seus dados para determinada finalidade. Neste cenário, na hipótese de o titular dar *opt-out* em relação ao recebimento do comunicado, pressupõe-se que ele não mais possuirá expectativa razoável para receber e-mails para a referida finalidade.

Dica! O tratamento de Dados Pessoais baseado no consentimento deve ser, sempre que possível, tido como exceção, considerando que a autorização pode ser retirada pelo titular.

COMO SOLICITAR ESSA AUTORIZAÇÃO?

Entre as formas de obtenção do consentimento para coleta de Dados Pessoais do titular e, consequente envio de comunicados, está o envio de e-mail questionando sobre a permissão de envio de convites, newsletter ou eventos futuros. **Mas lembre-se: a autorização pelo usuário deve anteceder o início do tratamento de Dados pela empresa.** De maneira simples, deve-se questionar antecipadamente se o usuário permite este tratamento de seus Dados Pessoais ou não.

Além disso, no website pode ser acrescentado um formulário de cadastro para o usuário solicitar o recebimento de newsletter ou informações sobre os serviços fornecidos pela empresa, e, por meio do preenchimento deste formulário, serão coletados os Dados e obtido o consentimento do usuário, caso seja essa a Base Legal aplicável.

É imprescindível, ainda, que sejam observados todos os requisitos exigidos pela LGPD para que o consentimento seja válido.

Tenha certeza em coletar o consentimento daqueles que já estão em sua base de Dados, quando esta for a única Base Legal aplicável.

Por exemplo, ao enviar um convite para um evento ou webinar, solicite autorização (quando o consentimento for a Base Legal escolhida), conforme modelo abaixo:

Eu li e concordo com os Termos de Serviço, bem como entendo o conteúdo da Política de Privacidade (coloque hiperlink que direcione a estes documentos). No caso de dúvidas, poderei entrar em contato com o Encarregado através do e-mail xxxx.

Sim ***Não***

Autorizo que os meus Dados Pessoais sejam utilizados para envio de comunicados e convites de eventos realizados pelo XXXX, podendo, a qualquer momento, revogar esse consentimento, que foi dado por mim de forma livre, inequívoca e informada.

Sim ***Não***

* Vale ressaltar que o disposto acima é um mero exemplo, cabendo uma análise do caso em concreto.

PLATAFORMAS DE CONTROLE EM NUVEM - COMO DEVE SER FEITO O ARMAZENAMENTO DAS INFORMAÇÕES E BASES CADASTRAIS E POR QUANTO TEMPO?

É imprescindível definir empregados autorizados que poderão tratar esses Dados Pessoais, bem como um local adequado para armazenar essas informações, criando-se, assim, um local seguro e mais protegido.

O armazenamento em plataformas, como SCS e Micromust, também precisam de cautela e atenção, para, além de conter somente os Dados Pessoais necessários, sempre manter as bases atualizadas e limitadas ao acesso.

Fora isto, é fundamental que se verifique o nível de observância à LGPD de prestadores de serviços contratados para gerir ou fornecer eventual plataforma e ferramenta de gerenciamento de banco de Dados, considerando que muitas vezes essas bases de Dados (clouds) estarão, inclusive, em outro país, ocorrendo, dessa forma, uma transferência internacional de Dados Pessoais, sob o aspecto da LGPD. Essa garantia de proteção deve constar em cláusulas contratuais específicas, devendo ser verificada, inclusive, a necessidade de elaboração de contratos/aditivos contratuais para adequação à LGPD.

Além disso, sugere-se a realização de uma ***Tabela de Temporalidade***, documento que contemplará os prazos de guarda, decorrentes de lei, bem como o enquadramento das atividades em Base Legal pertinente, para auxílio do Encarregado quanto ao armazenamento ou exclusão dos Dados Pessoais (verifique o Capítulo 4, na página 38).

4.2.3. COMO REGULAMENTAR AS RELAÇÕES COM PARCEIROS

No que diz respeito às relações contratuais em geral, em primeira análise, pode-se ter a errônea impressão de que não haverá o tratamento de Dados Pessoais, por exemplo, quando estamos diante de um contrato de parceria.

Contudo, uma vez que Dado Pessoal é toda e qualquer informação relacionada à pessoa natural identificada ou identificável, em sua maioria, os contratos trarão em seu conteúdo ou implicarão em seu objeto o tratamento e compartilhamento de Dados Pessoais entre as partes. Informações de representantes legais constantes em documentos que servem para elaborar um contrato, e até mesmo os Dados daqueles que assinam um contrato, merecem especial atenção por se enquadrarem no conceito de Dados Pessoais, passíveis de proteção sob o olhar da LGPD.

Inicialmente, é indicado realizar um mapeamento completo das parcerias e dos contratos em vigor e organizar os documentos atrelados, como os de representantes legais, para rever a adequação destes perante a LGPD.

Analise os contratos, entenda se de fato há o tratamento e/ou compartilhamento de Dados Pessoais entre as partes – e se há Dados sensíveis, inclusive -, quais as finalidades deste tratamento/compartilhamento e quais as Bases Legais que o autorizam.

Ainda, é essencial verificar qual das partes cumprirá o papel de Controlador e Operador (ou mesmo alguma outra figura definida pela ANPD) naquela atividade para que se defina corretamente as responsabilidades de cada Agente de Tratamento (no caso de dúvidas, consulte novamente o glossário exemplificativo).

Importante: a definição do Agente de Tratamento, ou seja, quem é o Operador e quem é o Controlador, estará vinculada a cada atividade exercida em específico. Em outras palavras, por ser um conceito dinâmico, em uma mesma relação contratual, cada parte poderá desempenhar em cada momento um papel diferente de Agente de Tratamento, de acordo com a atividade exercida.

Assim, deve-se buscar analisar as atividades-fim do contrato, de forma a estabelecer para cada uma delas a posição da entidade como Controladora ou Operadora. Essa classificação é relevante, pois determina o nível de responsabilidade de cada um dos Agentes de Tratamento nos casos de dano (patrimonial ou moral, individual ou coletivo) que decorram de descumprimento à Lei.

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. **Assim, todos os contratos analisados, novos ou antigos, devem conter novas cláusulas que os ajustem às regras e disposições da LGPD.**

As cláusulas de proteção de Dados devem, minimamente, abordar:

- Definição dos papéis das partes entre Operador e Controlador(ou mesmo alguma outra figura definida pela ANPD);
- Separação de responsabilidades entre as partes do contrato, com a disposição de métodos de auditoria e até mesmo possíveis sanções e punições no caso do desrespeito à legislação;
- Estabelecimento das finalidades e dos limites para a utilização dos Dados Pessoais envolvidos no contrato;
- Padrões e exigências mínimas de medidas de segurança, técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;
- Compartilhamento/Transferência de Dados Pessoais em território nacional e/ou internacional definida em cláusulas específicas;
- Garantia de que a empresa parceira tratará os Dados Pessoais recebidos com a mesma diligência que a entidade;
- Estabelecimento de premissas para a cooperação entre Controlador e Operador.

** As cláusulas e seu conteúdo deverão ser calibrados e melhor definidos a depender dos papeis dos Agentes de Tratamento naquela relação.*

É NECESSÁRIA UMA DEFINIÇÃO CONTRATUAL PARA REGER PARCERIAS? E SE INCLUÍREM COMPARTILHAMENTO/TRANSFERÊNCIA DE DADOS PESSOAIS?

Conforme previsto pela LGPD, o tratamento de Dados Pessoais envolve toda operação realizada com Dados Pessoais, como coleta, armazenamento, processamento e compartilhamento. A definição, portanto, já indica que uma entidade que recebe Dados Pessoais de outra, mesmo que não os tenha coletado diretamente do titular, também deve estar atenta ao disposto na nova Lei.

Como indicado anteriormente, é importante verificar as atribuições das partes envolvidas no tratamento de Dados, descrevendo em cláusula específica as responsabilidades de cada Agente de Tratamento. Além disso, é necessário descrever, em cláusulas específicas também, a finalidade do tratamento dos Dados Pessoais envolvidos e, se houver compartilhamento, descrever a Base Legal adequada para tanto, coletando o consentimento, se aplicável.

Abaixo, uma sugestão de Cláusula para compartilhamento de Dados Pessoais:

Cláusula XXX – Compartilhamento de Dados Pessoais (sem transferência internacional)

A {X – VERIFICAR AGENTE DE TRATAMENTO} assegurará que os Dados Pessoais não sejam acessados, compartilhados ou transferidos para terceiros (incluindo subcontratados, agentes autorizados e afiliados) sem o consentimento prévio por escrito da {X – VERIFICAR AGENTE DE TRATAMENTO}. Caso a {X – VERIFICAR AGENTE DE TRATAMENTO} autorize estas operações de tratamento, a {CONTRATADA} deverá garantir que tais terceiros se obriguem, por escrito, a garantir a mesma proteção aos Dados Pessoais estabelecida neste Contrato. A {X – VERIFICAR AGENTE DE TRATAMENTO} será responsável por todas as ações e omissões realizadas por tais terceiros, relativas ao tratamento dos Dados Pessoais, como se as tivesse realizado.

Caso a {X – VERIFICAR AGENTE DE TRATAMENTO} seja legalmente obrigada a compartilhar tais informações, deverá empregar todos os esforços para informar o compartilhamento à {X – VERIFICAR AGENTE DE TRATAMENTO} imediatamente.

** Vale ressaltar que o disposto acima é um mero exemplo, cabendo uma análise do caso em concreto.*

É PRECISO INCLUIR CLÁUSULA CONTRATUAL DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS?

Conforme previsto na LGPD, art. 48, caput, já é dever do Controlador comunicar à Autoridade Nacional de Proteção de Dados e ao titular qualquer incidente de segurança relativo aos Dados Pessoais tratados que possa acarretar risco ou dano relevante ao titular. As definições sobre prazo, conteúdo e medidas a serem tomadas estão sob regulamentação da ANPD, a qual deve, em breve, definir os parâmetros para tal. Por ora, recomenda-se que, após a ciência do evento adverso e havendo risco relevante, a ANPD seja comunicada com a maior brevidade possível, sendo tal considerado a título indicativo o prazo de 2 (dois) dias úteis, contados da data do conhecimento do incidente.

De qualquer forma, como medida protetiva e para conter danos e prejuízos, é recomendável a inclusão de uma cláusula no contrato de prestação de serviços a obrigação de o Controlador informar o mais rapidamente possível quando da ocorrência de qualquer incidente de segurança da informação envolvendo Dados Pessoais, bem como eventual cooperação entre as Partes para que seja possível o quanto antes a adoção de medidas de mitigação e estabelecimento de um fluxo a ser observado para o atendimento do exigido pela LGPD.

Abaixo, uma sugestão de Cláusula para Comunicação de Incidentes de Segurança:

Cláusula XXX – Dever de Comunicação de Incidentes

Na ocorrência de qualquer incidente (incluindo perda, deleção ou exposição, quer indesejada, não autorizada, ou maliciosa) que envolva as informações tratadas em razão da presente relação contratual, deverá a {OPERADORA} comunicar imediatamente à {CONTROLADORA}, inclusive cooperando com os esforços de investigação e remediação da {CONTROLADORA}, se comprometendo, ainda, a fornecer qualquer tipo de documento e informação solicitada pela {CONTROLADORA} com o intuito de mitigar os referidos danos. A comunicação, em caso de incidentes, deverá transmitir ao Encarregado da {CONTROLADORA} todas as informações conhecidas do evento e não menos do que: (i) a descrição dos Dados envolvidos (ii) a causa do evento, seja conhecida seja especulada, e a data de descoberta do incidente, além de (iii) o tipo e a quantidade de titulares de Dados afetados pelo evento por meio dos seguintes canais oficiais de comunicação

{canal de comunicação email@email.com e/ou DDD + Telefone}.

** Vale ressaltar que o disposto acima é um mero exemplo, cabendo uma análise do caso em concreto.*

AO FINAL DE UMA PARCERIA, EM QUE HOUVE TRANSFERÊNCIA DE DADOS, O PARCEIRO AINDA PODERÁ UTILIZAR ESSAS INFORMAÇÕES PARA SUAS CAMPANHAS PRÓPRIAS?

Nos contratos de parceria que envolvem transferência/compartilhamento de Dados Pessoais, a finalidade do tratamento dos Dados deve ser específica e estar descrita, bem como há a necessidade de que se defina o papel de Agente de Tratamento (Operador e Controlador) de cada uma das partes daquele contrato em relação às atividades desenvolvidas.

Desta forma, se a finalidade do compartilhamento de informações é para contemplar somente o período de vigência da parceria, sem que haja, por exemplo, uma lei (Base Legal de obrigação legal ou regulatória) que obrigue o Agente de Tratamento em questão a armazenar esses Dados mesmo após o término da relação contratual, é importante que ao final da parceria os Dados relativos ao banco de Dados da outra parte sejam descartados e não sejam utilizados em campanhas próprias, respeitando os princípios da LGPD, a transparência ao titular e a Base Legal utilizada.

Além disso, a todo momento, é imprescindível que se dê a devida transparência ao titular quanto ao tratamento e compartilhamento de seus Dados por meio de documento como o Aviso de Privacidade.

4.3. RELAÇÕES ADMINISTRATIVAS

4.3.1. COMO ADMINISTRAR RELAÇÕES COM TERCEIROS

Como mencionado anteriormente, no item 4.2.3, a vigência da LGPD exige a revisão dos contratos com terceiros, principalmente quando há o compartilhamento e tratamento de Dados Pessoais entre as partes. O contrato deve incluir as obrigações da empresa e do terceiro, de acordo com as regras e princípios contemplados pela LGPD. É necessário destacar, por exemplo, o não desvio da finalidade do tratamento de Dados Pessoais e a constante transparência ao titular, principalmente quando há o compartilhamento de seus Dados Pessoais com outro Agente de Tratamento – a exemplo de empresas prestadoras de serviços -, além dos procedimentos a serem observados no caso de eventual incidentes de segurança.

Além disso, quando houver o tratamento dos Dados Pessoais de pessoas físicas empregadas como mão-de-obra na prestação de serviços terceirizados, por exemplo, deverá constar no contrato de prestação de serviços cláusula que defina as obrigações das duas partes quanto ao tratamento dos Dados Pessoais daquela relação, bem como que se defina os procedimentos de segurança preventivos e os protocolos a serem adotados em caso de eventuais incidentes.

Ademais, para garantir de forma prévia uma observância ainda mais completa dos aspectos a serem verificados na relação com essa empresa terceira, sugere-se que se responda às seguintes perguntas.

Tais perguntas podem inclusive ser utilizadas para guiar os contratos firmados em sede do Tópico 4.2 deste Guia – Relações Comerciais.

- Esse terceiro adota/adotou processos e medidas que demonstrem que esteja em conformidade com a LGPD?
- É realmente necessário compartilhar estes Dados Pessoais com este terceiro?
- Esse terceiro, eventualmente, fará o tratamento destes Dados Pessoais compartilhados fora do Brasil?
- Todos os Dados Pessoais que pretendo compartilhar e que estarão envolvidos nessa relação são indispensáveis para atingir o objetivo requerido?
- Esta atividade e este Compartilhamento de Dados Pessoais estão no Registro de Atividades de tratamento de Dados da entidade?
- Tenho em mente as regras que deverão ser estabelecidas no contrato (ou outro instrumento jurídico relevante) com este terceiro?
- O Encarregado está ciente (ou precisa estar ciente) desse tratamento/compartilhamento?

Após esta análise:

- Classifique os contratos vigentes, caso já existentes, por nível de risco segundo a LGPD, com auxílio do Encarregado, fazendo as adequações necessárias. Se ainda não elaborada a classificação, peça auxílio ao departamento jurídico;
- Classifique seus fornecedores para sempre saber qual o grau de adequação à Política de Proteção e Privacidade de Dados;
- Veja se é necessário a realização de algum treinamento de manuseio de Dados Pessoais com esse Terceiro (principalmente quando ele ficará alocado nas dependências da entidade) ou alguma outra diligência prévia;
- Utilize um sistema de gestão de terceiros adequado à LGPD, caso entenda pertinente, mas sempre mantenha o Registro de Atividades de tratamento atualizado.

É SEMPRE RECOMENDÁVEL A ELABORAÇÃO DE CONTRATO ESCRITO COM PRESTADORES DE SERVIÇOS (EX. ESCRITÓRIOS ESPECIALIZADOS, PRESTADORES PJ COM PROFISSIONAL ALOCADO NAS DEPENDÊNCIAS DA EMPRESA, EMPRESAS DE BENEFÍCIOS, CONTABILIDADE...)?

Diante da existência de Dados Pessoais, para que não ocorra nenhum tratamento/compartilhamento sem Base Legal adequada que os justifiquem, igualmente como se estabelece com as parcerias (item 4.2.3), os contratos de prestação de serviço devem conter cláusulas específicas de proteção de Dados Pessoais para conduzir o tratamento e as responsabilidades de cada Agente de Tratamento sobre os Dados, bem como para que se estabeleça os critérios e padrões mínimos para condução das atividades objeto do contrato.

- No caso de compartilhamento/transferência de Dados Pessoais com empresas de Benefícios, é importante que a empresa dê a devida transparência aos titulares sobre os Dados Pessoais que são tratados/compartilhados com esses terceiros e para qual finalidade. Se verificado o consentimento como Base Legal mais adequada para o tratamento da atividade de Benefícios em si, considerando haver um compartilhamento com empresa terceira, faz-se necessária a coleta de uma autorização específica para tanto. Contudo, caso o compartilhamento se dê em razão do contrato prévio firmado com a empresa, por exemplo, que já previa a concessão desses Benefícios, nenhum consentimento é necessário neste caso, já que o compartilhamento estará embasado em outra Base Legal (execução de contrato).

É NECESSÁRIO CONSTAR NO CONTRATO FIRMADO COM O TERCEIRO UMA CLÁUSULA DE RESPONSABILIDADE E DE TRATAMENTO DAS INFORMAÇÕES?

É importante, no momento da elaboração e/ou formalização dos contratos, delimitar as responsabilidades de cada parte quanto às atividades de tratamento de Dados Pessoais envolvidas naquela relação, isso porque, uma vez que, por terem papéis diferentes no tratamento de Dados Pessoais, a responsabilidade do Controlador e do Operador também será diferente.

Inicialmente, vale destacar que tanto o Controlador quanto o Operador que, em razão das atividades de tratamento de Dados Pessoais, causarem danos patrimoniais, morais, individuais ou coletivos, serão **obrigados** a reparar/indenizar os titulares de Dados Pessoais envolvidos.

O Operador responderá **solidariamente** pelos danos causados quando descumprir as obrigações da LGPD ou quando não seguir as orientações lícitas do Controlador. Logo, se o Operador apenas cumprir determinações lícitas que lhe são passadas pelo Controlador, terá a responsabilidade afastada.

Do outro lado, considerando que o Controlador é quem toma as decisões acerca do tratamento de Dados, ele terá, consequentemente, maior responsabilidade, pois além de responder pelas próprias inobservâncias legais e danos que vier a causar, também responderá **solidariamente**, quando estiver **diretamente** envolvido no tratamento de Dados Pessoais do qual decorra violações à legislação e/ou danos causados pelo Operador.

Os Agentes de Tratamento, só não serão responsabilizados quando provarem que não realizaram o tratamento ilícito de Dados Pessoais atribuído a eles, que não houve violação à LGPD ou quando, por exemplo, verifica-se que o dano é decorrente de culpa exclusiva do titular dos Dados Pessoais ou de terceiros.

Dessa forma, eventuais descumprimentos da legislação por empresa terceirizada e/ou fornecedor que realize serviços que envolvam o tratamento de Dados Pessoais, como recepção predial, por exemplo, podem trazer prejuízos reputacionais e financeiros à empresa, razão pela qual é importante que a empresa fiscalize com rigor o cumprimento da legislação por seus terceirizados.

Importante: sempre que o Operador utilizar Dados Pessoais recebidos do Controlador para outra finalidade que não aquela que lhe foi inicialmente determinada/instruída, o Operador será considerado Controlador e, portanto, terá a sua responsabilidade ampliada. Esta situação será entendida como uma violação à LGPD por desvio da finalidade original dos Dados indicadas pelo Controlador e/ou por inobservância de cláusulas de limitação de uso do contrato entre as partes. Logo, para além dos cuidados internos que as instituições devem tomar para estarem adequados à LGPD, é imprescindível que os contratos firmados com terceiros definam as responsabilidades e obrigações de cada uma das partes no processo de tratamento de Dados Pessoais.

4.3.2. COMO TRATAR DADOS PESSOAIS DE REPRESENTANTES LEGAIS/PROCURADORES

QUAIS INFORMAÇÕES PODEM SER MANTIDAS NO BANCO DE DADOS E COMO ARMAZENAR ESTES DADOS?

Lembre-se sempre: representantes legais e procuradores são pessoas físicas e, portanto, proprietários (titulares) de seus Dados Pessoais.

Assim, informações de representantes legais constantes em seus documentos pessoais utilizadas para elaboração de contrato, assim como os Dados daqueles que assinam um instrumento jurídico, merecem especial atenção por se enquadrarem no conceito de Dados Pessoais, passíveis de proteção sob o olhar da LGPD.

De toda forma, novamente, a LGPD não prevê a descrição de quais Dados Pessoais podem ser solicitados a esses titulares, podendo, portanto, variar a depender das características e necessidades requeridas na relação jurídica. As finalidades e informações acerca deste tratamento devem estar disponíveis de maneira clara ao titular, assim como deve se ter em mente a obtenção apenas dos Dados mínimos e necessários para a finalidade específica, e pautando-se no enquadramento de uma Base Legal adequada para o tratamento.

Por exemplo, os Dados Pessoais, como nome, endereço residencial, documentos de identificação e telefone devem ser protegidos.

Exemplo: O tratamento de Dados Pessoais para a elaboração e posterior publicação dos contratos celebrados com órgãos públicos está respaldado no fundamento de obrigação legal ou regulatória, já que há previsão legal da publicação desses documentos, exigindo o tratamento de determinados Dados Pessoais para atingimento dessa finalidade. O mesmo fundamento também se aplica no caso da empresa que guardar Dados Pessoais de ex-empregado pelo prazo necessário para a defesa em processo trabalhista, por exemplo.

A aplicação da LGPD tem um impacto direto na manutenção dos Bancos de Dados, uma vez que devem ser mantidas as informações somente por um determinado período, enquanto necessárias para atingimento da finalidade anteriormente prevista e desde que fundamentadas por Base Legal adequada. Contudo, o armazenamento de Dados Pessoais de procuradores e representantes, como regra geral, ocorre por atender interesses legítimos do Controlador para o apoio e promoção de suas atividades e para o cumprimento de obrigações decorrentes de lei, podendo, desse modo, haver o enquadramento, respectivamente, na Base Legal do legítimo interesse e obrigação legal ou regulatória.

As empresas que ainda mantém informações em arquivos físicos podem sofrer ainda mais com as regras da LGPD. É interessante, se este for o caso, pensar na digitalização e automatização do processo, para facilitar a gestão de documentos, tornando-a mais segura, e eficiente e até mais rápida, inclusive para atender titulares que venham a exercer direitos advindos da LGPD.

No mais, quanto ao quesito da transparência ao titular, sugere-se que estas informações estejam disponíveis no Aviso de Privacidade - quanto tempo essas informações ficarão armazenadas no Banco de Dados, se haverá algum tipo de compartilhamento, para qual finalidade e qual a Base Legal que autoriza o tratamento de Dados.

A LGPD PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

A LGPD PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

Em reconhecimento da importância de uma regulação específica para Agentes de Tratamento de pequeno porte e em conformidade com o artigo 55-J, inciso XVIII, da Lei Geral de Proteção de Dados Pessoais (LGPD), a Autoridade Nacional de Proteção de Dados (ANPD) publicou, em 27 de janeiro de 2022, a sua Resolução CD/ANPD nº 2 a fim de estabelecer diretrizes para Agentes de Tratamento de pequeno porte, nos termos da lei.

Destacamos que a FIESP e o CIESP têm defendido o tratamento diferenciado para microempresas e empresas de pequeno porte em todas as frentes de atuação e participaram da tomada de subsídios da ANPD para a elaboração da Resolução mencionada, com diversas contribuições incorporadas ao seu texto final.

Ademais, o tratamento diferenciado aos agentes de pequeno porte reflete a importância e o entendimento expressos na Nota Técnica nº1/2021/CGN/ANPD, emitida em janeiro de 2021 pela ANPD, de que a redução da carga regulatória e o estímulo à inovação são fatores fundamentais para o desenvolvimento das microempresas e empresas de pequeno porte e, consequentemente, para o país, destacando a liberdade como garantia no exercício de atividades econômicas e a intervenção subsidiária e excepcional do Estado sobre o exercício de atividades econômicas. É nesse contexto que se justifica a Resolução CD/ANPD nº2.

5.1. A QUEM SE APLICA?

Por Agentes de Tratamento de pequeno porte se entende as microempresas, empresas de pequeno porte, *startups* e empresas de inovação, bem como as pessoas físicas que tratem Dados Pessoais com fins econômicos (At. 2º, I). A ANPD traz definições importantes sobre tais agentes que delimitarão quais pessoais físicas e jurídicas poderão se beneficiar do tratamento diferenciado. Conforme legislação vigente, entende-se por:

- Microempresas e empresa de pequeno porte: "sociedade empresária, sociedade simples, sociedade limitada unipessoal, nos termos do art. 41 da Lei nº 14.195, de 26 de agosto de 2021, e o empresário a que se refere o art 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual [MEI] [...]" (Art. 2º, II).

- Startups: "organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados que atendam aos critérios previstos no Capítulo II da Lei Complementar nº 182, de 1º de junho de 2021" (Art. 2º, III).

Da mesma forma, e tendo em vista a segurança jurídica de Agentes de Tratamento e titulares dos Dados Pessoais, a ANPD estabelece algumas condicionantes para tratamento jurídico específico. De acordo com a Autoridade, não poderão se beneficiar do tratamento jurídico diferenciado os Agentes de Tratamento de pequeno porte que:

- Realizem tratamento de alto risco para titulares (Art. 3º, III).
- Aufiram receita bruta superior ao limite estabelecido no art. 3°, II, da Lei Complementar 123, de 2006 ou, no caso das startups, no art. 4° $1º, I, da Lei Complementar n 182, de 2021 (Art. 3º, II).
- Pertençam ao grupo econômico de fato ou de direito, cuja receita global ultrapasse os limites referidos no inciso II, conforme o caso (Art. 3º, III).

Os limites de receita definidos se referem, respectivamente, ao Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte e ao Marco Legal das Startups. Portanto, o limite geral, para microempresa e para empresas de pequeno porte é de, respectivamente R$ 360.000,00 e R$ 4.800.000,00. Já no tocante às startups, prevê-se, independentemente da forma societária, receita bruta de até R$ 16.000.000,00, no ano-calendário anterior ou então de R$ 1.333.334,00 multiplicado pelo número de meses de atividade, no ano-calendário anterior, se inferior a 12 meses.

Por sua vez, o tratamento de alto risco é definido conforme o Art. 4º da Resolução CD/ANPD nº 2, como o tratamento de Dados Pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, conforme listado:

Critérios Gerais:

- Tratamento de Dados Pessoais em larga escala – abrangendo número significativo de titulares, considerando ainda o volume de Dados, a duração, frequência e extensão geográfica do tratamento;
- Tratamento de Dados Pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares – a exemplo de atividade de tratamento que impeça o exercício de direitos ou a utilização de um serviço, ou que ocasione danos materiais ou morais (discriminação, violação à integridade física etc.);

Critérios específicos

- Uso de tecnologias emergentes ou inovadoras;
- Vigilância ou controle de zonas acessíveis ao público (praças, centros comerciais, vias públicas, estações de metrô e ônibus, dentre outros);
- Decisões baseadas unicamente em tratamento automatizado de Dados Pessoais, inclusive as destinadas a definir o perfil pessoal, profissional, de saúde, consumo e de crédito ou os aspectos da personalidade do titular;
- Utilização de Dados Pessoais sensíveis ou de Dados Pessoais de crianças, de adolescentes e de idosos.
- Para auxiliar na avaliação do tratamento de alto risco a ANPD indica em sua Resolução que poderá disponibilizar guias e orientações aos Agentes de Tratamento de pequeno porte.

A ANPD estabelece ainda, a responsabilidade ao Agente de Tratamento de pequeno porte, caso solicitado pela ANPD, a comprovação de seu enquadramento nos requisitos e condicionantes acima listados e nos demais termos da Resolução, no prazo de até 15 (quinze) dias após a solicitação.

É importante esclarecer, entretanto, que a flexibilização ou dispensa de obrigações a tais Agentes, que apresentaremos a seguir, não deve ser tomada como isenção do cumprimento dos demais dispositivos da LGPD. Em outras palavras, os Agentes de Tratamento de pequeno porte deverão se atentar ao cumprimento dos demais dispositivos da LGPD e de outras disposições legais, regulamentares e contratuais referentes à proteção de Dados Pessoais, assim como aos direitos dos titulares.

5.2. DAS OBRIGAÇÕES

A ANPD prevê como obrigação que o Agente de Tratamento de pequeno porte disponibilize informações sobre o tratamento de Dados Pessoais e atenda às requisições dos titulares por meio eletrônico, impresso ou qualquer outro que assegure os direitos previstos na LGPD e o acesso facilitado pelos titulares (Art. 7º).

Faculta aos agentes que se organizem por meio de entidades de representação da atividade empresarial (Art. 8º), assim como designa que o cumprimento da obrigação de elaboração e manutenção de registro das operações de tratamento de Dados Pessoais, previso no art. 37 da LGPD, poderá se dar de forma simplificada, conforme modelo para registro a ser fornecido pela Autoridade (Art. 9º).

Ademais, a Resolução indica que a ANPD irá dispor acerca da flexibilização ou procedimento simplificado de comunicação de incidente de segurança para os Agentes de Tratamento de pequeno porte (Art. 10).

5.3. DA NOMEAÇÃO DO ENCARREGADO

Dispensa a obrigatoriedade de o Agente de Tratamento de pequeno porte nomear um Encarregado pelo tratamento de Dados Pessoais (DPO). Todavia, exige, em caso de dispensa, a disponibilização de um canal de comunicação direto entre o Agente de Tratamento e o titular dos Dados Pessoais. Em caso de indicação de Encarregado, a nomeação será tomada como um mecanismo de boas práticas para os fins do artigo 52, parágrafo 2º, inciso I, da LGPD (Art. 11).

5.4. DA SEGURANÇA E BOAS PRÁTICAS

A ANPD exige dos Agentes de Tratamento de pequeno porte a adoção de medidas administrativas e técnicas a fim de garantir a segurança da informação e proteção dos Dados Pessoais. Nesse sentido, o atendimento às recomendações e boas práticas divulgadas pela ANPD será considerado como observância ao art. 52, § 1º, inciso VIII da LGPD, sobre adoção de mecanismos voltados ao tratamento seguro de Dados (Art. 12).

Ainda, a Resolução prevê que tais agentes poderão estabelecer política simplificada de segurança da informação, contemplando os requisitos para o tratamento de Dados Pessoais, observando sempre a proteção dos mesmos e considerando os custos de implementação, estrutura, escala e volume das operações do agente. Sua adoção será considerada pela ANPD para fins dos art. 6º, X, sobre responsabilização e prestação de contas, e do art. 52, § 1º, inciso VIII, já citado, e IX, sobre políticas de boas práticas e governança (Art. 13).

5.5. PRAZOS ESPECÍFICOS

A ANPD, em seu artigo 14, concede prazo diferenciado aos Agentes de Tratamento de pequeno porte, ressaltando que, para quaisquer prazos não dispostos na Resolução CD/ANPD nº 2, haverá determinação em regulamentação específica posterior.

Neste sentido, a Resolução determina que os prazos estabelecidos nos normativos próprios da ANPD para apresentação de informações, documentos, relatórios e registros solicitados terão **prazo dobrado** aos Agentes de Tratamento de pequeno porte em relação aos demais.

O quadro abaixo traz um breve, porém importante, resumo dos diferentes prazos estabelecidos.

PRAZOS DEFINIDOS PELA LGPD E PELA RESOLUÇÃO CD/ANPD Nº 2		
Exigência	**Agentes de Tratamento de Pequeno Porte**	**Demais Agentes de Tratamento**
Atendimento de solicitação dos titulares (com exceção do direito de confirmação e acesso)	Dobro dos prazos pendentes de regulamentação	Prazos pendentes de regulamentação
Comunicação de incidente de segurança, ao titular e à ANPD*	4 dias úteis	2 dias úteis**
Fornecimento de declaração clara e completa (direito do titular de confirmação de existência ou o acesso) * **	30 dias	15 dias
Declaração simplificada (direito do titular de confirmação de existência ou o acesso), quando requerida pelo titular* **	Até 15 dias a partir do requerimento do titular	Imediato, mediante solicitação

* Exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional, caso em que a comunicação deverá seguir o parâmetro indicado aos demais agentes de tratamento (Art. 14, II).

** A LGPD designa que a comunicação deverá ser feita em "prazo razoável" a ser definido pela ANPD. Todavia, tal definição ainda não foi realizada, sendo o prazo de 2 (dois) dias úteis o indicativo de boas práticas existente no site da Autoridade. Ver https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

*** Prevista no Art. 19, II, da LGPD.

**** Prevista no Art. 19, I, da LGPD.

PERGUNTAS FREQUENTES (FAQ)

PERGUNTAS FREQUENTES (FAQ)

1. EM LINHAS GERAIS, O QUE SE DEVE SABER SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS?

O QUE DEVE SER FEITO?	Deve ser realizada a adequação de todos os processos internos relacionados ao tratamento de Dados Pessoais – veja novamente o **Capítulo 1**.
POR QUÊ?	A LGPD tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural e, nesse contexto, visa proteger os Dados Pessoais ao determinar diretrizes para o tratamento de Dados Pessoais dos indivíduos.
ONDE?	Em todas as áreas da organização que tratam Dados Pessoais no desenvolvimento de suas atividades e cujas empresas estejam sob escopo de aplicação da LGPD.
QUANDO?	A Lei entrou em vigor em 18 de setembro de 2020, mas a aplicação das sanções administrativas previstas na legislação teve início a partir de 1º de agosto de 2021.
QUEM SÃO AS PRINCIPAIS PARTES ENVOLVIDAS?	A LGPD conceitua, entre outras, as seguintes partes que possuem direitos ou deveres relacionados aos Dados Pessoais: o titular dos Dados Pessoais (indivíduos – pessoas físicas), o Operador, o Controlador, o Encarregado e a ANPD – veja as definições no **Capítulo 2**.
COMO?	As atividades de tratamento de Dados Pessoais devem respeitar os requisitos, a boa-fé e os princípios estabelecidos na Lei. Cada organização deve analisar se essas exigências estão sendo observadas internamente - veja novamente o **Capítulo 3**.
QUANTO VAI CUSTAR?	Os processos para adequação aos requisitos de proteção dos dados e privacidade, com responsabilidade social e prevenção de incidentes devem ser considerados como um investimento estratégico. O custo da não adequação deve ser avaliado, em razão do risco de prejuízos legais, financeiros e até mesmo reputacionais. O mero descumprimento da LGPD já caracteriza infração, passível, portanto, das sanções aplicáveis.

2. POR ONDE DEVO COMEÇAR E O QUE PRIORIZAR? AINDA HÁ TEMPO PARA A ADEQUAÇÃO?

Inicialmente, vale lembrar que a adequação é contínua. A LGPD entrou em vigor em setembro de 2020 e, considerando que as sanções administrativas passaram a vigorar em 1º de agosto de 2021, é importante atentar que ações judiciais já têm sido propostas levando em conta aspectos da LGPD. As empresas devem ponderar e levar em consideração em suas respectivas adequações, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de Dados que lhes competem.

Não há um caminho único a ser seguido para se adequar à LGPD, porém, alguns pontos são importantes, como mapear os dados e identificar sua posição enquanto Agente de Tratamento daquelas atividades, compreender as Bases Legais para tratamento de Dados Pessoais, de maneira geral, (verifique o Capítulo 1, na página 08) e identificar as áreas dentro de sua empresa que tratam esses Dados Pessoais e se há, por exemplo, Dados Pessoais sensíveis sendo tratados. Como sugestão, apresentamos no **Capítulo 3 os Principais Passos para Adequação**, no qual se pode verificar uma ordem de atividades a serem realizadas que, se observadas, poderão colocar sua entidade em uma posição favorável frente aos desafios impostos pela Lei.

3. QUAIS OS MAIORES RISCOS DA UTILIZAÇÃO INDEVIDA DE DADOS PESSOAIS? E COMO OCORRERÁ A FISCALIZAÇÃO?

A fiscalização será realizada pela Autoridade Nacional de Proteção de Dados (ANPD), o órgão federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD e cujas sanções administrativas passaram a vigorar a partir de 1º de agosto de 2021. É importante, contudo, que se verifique as especificidades quanto a este tema contempladas no Tópico 1.2 deste Guia, especialmente quanto ao início do processo de fiscalização em si.

Desta forma, os Agentes de Tratamento de Dados que cometerem infrações às disposições previstas na Lei, ficam sujeitos a distintas sanções administrativas, como multas que podem chegar a 50 milhões de reais por infração (verifique o Capítulo 1 para mais informações). Ademais, danos reputacionais à imagem da empresa e/ou de seus dirigentes também são riscos que podem levar, inclusive, à perda de parceiros, negócios e clientes.

Em suma, **o não cumprimento da LGPD pode gerar impactos legais, comerciais, financeiros e/ou reputacionais**, portanto, atente-se às indicações contempladas neste Guia e acompanhe as regulamentações e direcionamentos da ANPD.

4. DEVE-SE CONTRATAR PRESTADORES DE SERVIÇO E UM ENCARREGADO PARA ADEQUAÇÃO À LGPD?

Este Guia apresenta amplo conteúdo, com direcionamentos e orientações relativos à LGPD. Contudo, **é indicado mensurar o nível de dificuldade desta adequação e os respectivos riscos relacionados frente à quantidade de atividades e documentos a serem ajustados**, além do tamanho da base de Dados tratada em sua empresa. Caso sua entidade não tenha recurso suficiente (pessoal e/ou know-how) ou o processo de adequação seja dificultoso, recomenda-se a contratação de serviço externo para apoiar técnica e juridicamente

a adequação à LGPD, contando com especialistas em proteção de Dados para implementar todas as etapas de adequação e exigências da Lei.

Em relação ao Encarregado pelo Tratamento de Dados Pessoais, o porta-voz da empresa e centralizador de todas as ações necessárias à implementação de um projeto de adequação, pode ser qualquer pessoa, inclusive jurídica, contanto que tenha, no mínimo, conhecimento sólido sobre a Lei, regulamentações pertinentes e sobre as necessidades específicas e desafios da empresa. As competências e habilidades desejáveis de um Encarregado estão no **Subcapítulo 3.2 Estabeleça um Líder**. Caso não encontre profissional com estes requerimentos e competências técnicas, sugere-se a terceirização do serviço para que a empresa esteja bem representada.

Atenção! Lembre-se que este Guia Orientativo indica, de forma exemplificativa, os principais passos para a conformidade das atividades de tratamento de Dados pela empresa, e que, portanto, não tem a finalidade de esgotar a análise da matéria.

5. O QUE DEVE SER FEITO CASO UM TITULAR SOLICITE ACESSO AOS SEUS DADOS?

É essencial que se crie canais de comunicação tanto para contato com o Encarregado quanto para o exercício de direitos dos titulares, isto considerando que a LGPD traz, dentre esses direitos, o de confirmação da existência de tratamento, correção dos Dados inexatos ou eliminação, bem como se há compartilhamento dos Dados com terceiros.

Diante de uma requisição realizada por um titular acerca da confirmação da existência de tratamento de Dados Pessoais, por exemplo, a empresa deverá ter um processo interno definido para este atendimento. Assim, deverá ter mapeada as atividades de tratamento realizadas com os Dados Pessoais daquele indivíduo, para uma resposta breve e precisa, dentro do prazo legal. Desta forma, siga as orientações descritas no **Subcapítulo 3.3 estabeleça um Canal de Comunicação**.

6. SERÁ NECESSÁRIO ADAPTAR O ENVIO DE COMUNICADOS, MAILINGS, NEWSLETTERS E OUTROS NOS DIVERSOS CANAIS DE COMUNICAÇÃO (E-MAIL, *WHATSAPP*, *LINKEDIN*...)?

Caso a empresa tenha Dados Pessoais envolvidos nessas comunicações, será necessário, uma vez que, além de todos os princípios, a LGPD preza por uma relação transparente entre as partes, sendo, neste caso, fundamental, ainda, a existência de uma Base Legal que autorize o tratamento desses Dados Pessoais do titular. Em geral, para operações de comunicação (como envio de e-mail marketing, SMS e mensagens em distintas redes), envio de convites, promoções, notícias e outros, a Base Legal do consentimento será a mais adequada. Contudo, consulte o Encarregado para essa avaliação.

Para saber mais sobre como adequar os envios de comunicados a seus parceiros, clientes e outros, verifique o item **4.2.2 Envio de Informativos e Meios de Comunicação** deste Guia.

7. É PERMITIDO O COMPARTILHAMENTO LIVRE DE DADOS PESSOAIS (NOME, E-MAIL, TELEFONE, REDES SOCIAIS E OUTROS) A PARCEIROS, TERCEIROS OU EM PÁGINAS DA WEB? E DADOS CORPORATIVOS?

De acordo com os princípios elencados na LGPD, como o de adequação, finalidade e transparência, é preciso haver compatibilidade do tratamento com as finalidades informadas ao titular, ou seja, o titular sempre deverá estar ciente sobre o compartilhamento de seus Dados Pessoais a terceiros e as finalidades para tanto.

Lembre-se que não são considerados Dados Pessoais aqueles relativos a uma pessoa jurídica, como CNPJ, razão social e endereço comercial, desde que, a partir de tais informações, não seja possível identificar uma pessoa física. Assim, como regra geral, a LGPD não dispõe sobre o tratamento de Dados de pessoas jurídicas, mas, quando se referir aos Dados corporativos, como e-mail, telefone, ou Dados de representantes que permitam a identificação da pessoa física, a LGPD será aplicada.

8. SERÁ PRECISO ADEQUAR TODOS OS CONTRATOS, INCLUSIVE ANTIGOS?

Na maioria dos casos, os contratos e acordos implicarão no tratamento e/ou compartilhamento de Dados entre as partes, inclusive informação de representantes legais e Dados daqueles que assinam o documento.

É, portanto, indicado realizar um mapeamento completo das parcerias e dos contratos em vigor, e anteriores também, e organizar os documentos atrelados para rever a adequação perante a LGPD. Isso é um ponto importante, inclusive, para que se estabeleça as responsabilidades de cada Agente de Tratamento naquela relação. Encontre mais informações em **4.2.2 Como Regulamentar as Relações com Parceiros**.

9. COMO TRATAR DADOS DE FUNCIONÁRIOS E CURRÍCULOS ARMAZENADOS PELO SETOR DE RECURSOS HUMANOS?

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, na concessão de benefícios como plano de saúde, vale-refeição etc., ou até mesmo após eventual desligamento, sendo que, em cada uma destas etapas, deve-se analisar a finalidade do tratamento de Dados e enquadramento na Base Legal pertinente.

Além de definir empregados autorizados e local adequado para armazenamento das informações, é importante ser transparente com candidatos em relação às práticas e utilização de seus Dados Pessoais, por meio, por

exemplo, de Aviso de Privacidade ou outra forma aplicável, além de documentar a autorização de uso, se o consentimento for a Base Legal mais adequada. Veja o **Subcapítulo 4.1 Relações de Trabalho** para mais informações e detalhes.

10. COMO PROCEDER EM CASO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS?

O processo de adequação à LGPD, envolvendo toda a revisão sobre as atividades de tratamento dos Dados e enfoque na privacidade e proteção de dados em todos as atividades e documentos dentro de uma empresa, como elucidado neste Guia, é um movimento importante para proteger sua empresa e evitar incidentes de segurança envolvendo Dados Pessoais, sendo, inclusive, considerado um investimento estratégico.

Contudo, caso ocorra um incidente de segurança que possa acarretar risco ou dano relevante aos titulares em sua empresa, conforme descreve a Lei, o Controlador deverá comunicar à ANPD e ao titular sobre a ocorrência com a maior brevidade possível, sendo indicado o prazo de 2 (dois) dias úteis, contados da data do conhecimento do incidente. Encontre mais informações sobre notificação de incidentes no **Subcapítulo 1.2 A Autoridade Nacional de Proteção de Dados**.

FIESP | 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

Jorge Matheus Oliveira Rodrigues
Analista do Departamento de Defesa e Segurança da FIESP

Larissa Nunes Silva
Colaboradora do Grupo de Trabalho de Segurança e Defesa Cibernética

Maria Eduarda Annarumma Guedes
Colaboradora do Grupo de Trabalho de Segurança e Defesa Cibernética

COORDENAÇÃO

Clara Martinolli Freire da Silva
Gerente do Departamento de Defesa e Segurança da FIESP

Juliana Souza Mota
Coordenadora do Departamento de Defesa e Segurança da FIESP

FIESP CIESP