POLÍTICA GERAL DE PRIVACIDADE

Versão nº 1, criada em 19/09/2023

A presente Política de Privacidade (a "Política") explica de maneira clara e com linguagem de fácil compreensão a preocupação e adequação de **FERRANTE ADVOGADOS (TELPIS FERRANTE SOCIEDADE INDIVIDUAL DE ADVOCACIA)**, sociedade individual de advocacia, com registro sob nº 494.97 (OAB-SP) em relação a como são tratados os dados pessoais das pessoas físicas que eventualmente interajam com FERRANTE ADVOGADOS de forma que o tratamento de dados pessoais seja eventualmente necessário, em atendimento à Lei Geral de Proteção de Dados Pessoais – "LGPD" (Lei nº 13.709/2018 e alterações subsequentes), ou normas que eventualmente a tenha alterado, a altere ou a substitua, além das demais normas relacionadas à proteção de dados pessoais no Brasil.

1. QUEM, QUAIS, COMO E POR QUÊ?

O quadro abaixo apresenta um panorama em relação a quais são as pessoas que se submetem ao tratamento de dados pessoais do CONTROLADOR, quais são dados eventualmente tratados, como é feito o tratamento e quais suas finalidades:

VISITANTES DA FERRANTE ADVOGADOS:

DADOS REQUISITADOS/TRATADOS	SOLICITANTE USUAL	FINALIDADE	BASE LEGAL
CPF/RG ou, na sua falta, alguma informação de identificação da pessoa física Número de RG/CPF (ou, em sua impossibilidade, algum outro número de identificação de identidade, a critério do titular)	Recepcionista do prédio ou algum funcionário, sócio e/ou advogado responsável pelo ingresso da pessoa física no prédio	No caso de ingresso no prédio do escritório, o CPF/RG ou algum número de identificação da pessoa física é necessário para a segurança do prédio e daqueles que lá se encontram. Identificação do visitante e medidas de segurança do CONTROLADOR e dos próprios visitantes garantindo identificação das pessoas que nele ingressam e deixam o local, mitigando a	Necessário para o cumprimento de obrigação legal pelo CONTROLADOR – dever de segurança, conforme art. 22, §1º, b, da Lei dos Condomínios em Edificações e Incorporações imobiliárias – Lei nº 4.591/1964 – (art. 7º, II, LGPD) Necessário para atender interesses legítimos do CONTROLADOR, tais como segurança do imóvel e dos visitantes (art. 7º, IX, LGPD)

		hipótese pessoas sem identificação que eventualmente ingressem no local e eventualmente pratiquem atos contrários à legislação vigente no Brasil.	

POTENCIAIS CLIENTES OU CLIENTES EFETIVOS

DADOS REQUISITADOS/TRATADOS	SOLICITANTE USUAL	FINALIDADE	BASES LEGAIS:
Nome completo da pessoa física (ou, se a parte for pessoa física)	Ferrante Advogados, por meio de seus sócios, advogados e/ou alguém da equipe	Identificação das partes do Contrato	Necessário para a execução do contrato ou procedimentos preliminares (art. 7º, V, LGPD) Necessário para atender interesses legítimos do CONTROLADOR (art. 7º, IX, LGPD) Necessário para exercício regular de direitos em eventuais processos judiciais ou arbitrais (art. 7º, IX, LGPD) Necessário para o cumprimento de obrigação legal do CONTROLADOR – qualificação das partes – (art. 7º, II, LGPD)
Nome completo da pessoa jurídica (se a parte for pessoa jurídica)		Identificação das partes do Contrato	
Número de RG		Identificação das partes do Contrato	
Número de CPF		Viabilidade de correspondência entre as partes e exercício de eventuais direitos extrajudicialmente ou judicialmente	
Endereço de correspondência			
Telefone para contato			
E-mail		Qualificação das partes e necessidade para exercício regular de direitos e execução de contrato	

FUNCIONÁRIOS E/OU CANDIDATOS A FUNCIONÁRIOS DO CONTROLADOR

VIDE POLÍTICA DE RECURSOS HUMANOS RELACIONADA A PROTEÇÃO DE DADOS PESSOAIS AO FINAL DO PRESENTE DOCUMENTO

NEGATIVA DE FORNECIMENTO DE CONSENTIMENTO

O consentimento não é uma das bases legais utilizada no presente termo LGPD. Não obstante, em casos em que alguma das partes, para a execução de eventuais relações contratuais que impliquem em necessidade de consentimento, a negativa de fornecimento de consentimento, quando aplicável tal base legal, conforme quadro de finalidades e dados tratados, implicará ou poderá implicar no não acesso ao prédio, para visitantes, ou, em caso de contratantes e/ou relação contratual, impossibilidade de estabelecimento de relação contratual ou sua manutenção.

2. DIREITOS DOS TITULARES E DEVERES DE FERRANTE ADVOGADOS

A presente política tem por objetivo, conforme determinado na LGPD:

- Garantir o tratamento dos dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa física que de algum modo tenha seus dados tratados pelo CONTROLADOR, de acordo com o quanto especificado na presente política.
- Garantir o respeito aos seguintes direitos da pessoa física que de algum modo tenha seus dados tratados pelo CONTROLADOR, de acordo com o quanto especificado na presente política:
  - ✓ Respeito à privacidade;
  - ✓ Autodeterminação informativa, ou seja, o poder, controle e titularidade que cada cidadão tem sobre seus próprios dados pessoais;
  - ✓ liberdade de expressão, de informação, de comunicação e de opinião;
  - ✓ Inviolabilidade da intimidade, da honra e da imagem;
  - ✓ Desenvolvimento econômico e tecnológico e a inovação;
  - ✓ Livre iniciativa, a livre concorrência e a defesa do consumidor;
  - ✓ Direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais;
  - ✓ Finalidades específicas e informadas de tratamento de dados pessoais;
  - ✓ Forma e duração do tratamento, observados os segredos comercial e industrial;
  - ✓ Direito de fornecimento de identificação do CONTROLADOR;
  - ✓ Direito de acesso a informações de contato do CONTROLADOR;
  - ✓ Informações acerca do eventual uso compartilhado de dados pessoais e a finalidade, caso essa hipótese seja prevista na presente política
  - ✓ Responsabilidades dos agentes que realizarão o tratamento de dados pessoais;
  - ✓ Confirmação da existência de tratamento de dados pessoais;
  - ✓ Acesso a dados pessoais;
  - ✓ Correção de dados incompletos, inexatos ou desatualizados;
  - ✓ Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
  - ✓ Portabilidade dos dados a algum terceiros e/ou fornecedor de serviço ou produto, mediante requisição expressa do titular, de acordo com a regulamentação da LGPD e da autoridade nacional, observados os segredos comercial e industrial;

- ✓ Eliminação dos dados pessoais tratados com o consentimento do titular, quando aplicável tal base legal, exceto nas hipóteses previstas na LGPD, que são as seguintes mencionadas abaixo, sendo que os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: (i) cumprimento de obrigação legal ou regulatória do CONTROLADOR; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou (iv) uso exclusivo de CONTROLADOR, vedado seu acesso por terceiro, e desde que anonimizados os dados.
- ✓ Informação das entidades públicas e privadas com as quais o CONTROLADOR realizou uso compartilhado de dados;
- ✓ Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- ✓ Revogação do consentimento;
- ✓ Término do tratamento de dados pessoais, que ocorre nas seguintes hipóteses: (i) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) fim do período de tratamento; (iii) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme já explicado acima, resguardado o interesse público; ou (iv) determinação da autoridade nacional de proteção de dados (ANPD), quando aplicável.

Perceba que todos esses direitos, e os demais ora expostos, são explicados ao longo dessa Política, mas fique à vontade para contatar o DPO da CONTROLADOR no e-mail a seguir caso tenha ficado alguma dúvida: douglasferrante@ferranteadvogados.com

Além disso, a presente política tem por objetivo, conforme determinado na LGPD:

- Garantir que as atividades de tratamento de dados pessoais realizadas pelo CONTROLADOR respeitem os seguintes direitos da pessoa física que de algum modo tenha seus dados tratados pelo CONTROLADOR, de acordo com o quanto especificado na presente política, e observado os seguintes critérios e imposições pela LGPD:
  - ✓ Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
  - ✓ Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
  - ✓ Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
  - ✓ Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

- ✓ Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- ✓ Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- ✓ 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;
- ✓ Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- ✓ Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- ✓ Responsabilização e prestação de contas: demonstração, pelo agente, 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.

- Garantir que as atividades de tratamento de dados pessoais realizadas pelo CONTROLADOR respeitem as seguintes bases legais de tratamento aplicáveis efetivamente ou potencialmente, ou seja, hipóteses nas quais o tratamento de dados pessoais é permitido, conforme consta da LGPD, de modo a garantir a plenitude dos direitos da pessoa física que de algum modo tenha seus dados tratados pelo CONTROLADOR, de acordo com o quanto especificado na presente política:
  - ✓ Fornecimento de consentimento pelo titular;
  - ✓ Cumprimento de obrigação legal ou regulatória pelo controlador/CONTROLADOR;
  - ✓ Necessidade para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
  - ✓ Exercício regular de direitos em processo judicial, administrativo ou arbitral;
  - ✓ Proteção da vida ou da incolumidade física do titular ou de terceiro;
  - ✓ Necessidade para atender aos interesses legítimos do CONTROLADOR ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
  - ✓ Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Quanto ao tratamento de dados pessoais cujo acesso é público, caso isso venha a ocorrer, o CONTROLADOR obedecerá ao quanto disposto na presente Política, e agirá de acordo com a LGPD, sendo certo que o CONTROLADOR obedecerá a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. Será dispensada a exigência do consentimento mencionado para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na LGPD.

A eventual dispensa da exigência do consentimento não desobrigará o CONTROLADOR das demais obrigações previstas na LGPD, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Além disso, caso o tratamento posterior dos dados pessoais relativos aos dados pessoais públicos seja necessário para novas finalidades, haverá observância de propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na LGPD.

Em nenhuma hipótese o CONTROLADOR fará o tratamento de dados pessoais mediante vício de consentimento, quando a base legal para tratamento for consentimento.

O consentimento dos titulares, quando aplicável, conforme é explicado nessa Política, se relaciona com finalidades determinadas, com explicação de finalidade de cada dado pessoal obtido, sendo certo que o CONTROLADOR não fará utilização de autorizações contrárias à LGPD. A CONTROLADOR agirá para garantir totalmente os direitos dos titulares dos dados pessoais.

O consentimento dos titulares, quando aplicável, poderá ser revogado a qualquer momento mediante manifestação expressa, bastando requisição para o DPO do CONTROLADOR. São ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

Abaixo, apresenta-se uma lista dos principais direitos dos titulares dos dados pessoais eventualmente tratados conforme a presente Política.

Em caso de alteração de informação referida nos itens I, II, III ou V abaixo, quando aplicável, o CONTROLADOR informará de maneira pública e de fácil acesso – na entrada do estabelecimento do CONTROLADOR, com acesso público a todos os visitantes, com destaque de forma específica do teor das alterações, sendo que os titulares dos dados pessoais, nos casos em que o seu consentimento é exigido, poderão revogá-lo caso discorde da alteração.

Suas informações pessoais serão tratadas de forma confidencial. Não faremos tratamento indevido dos seus dados pessoais, exceto se exigido por lei ou ordem judicial, ou quando autorizado, quando aplicável a base legal de consentimento, conforme o quanto previsto abaixo nesta Política, em relação ao qual você se declarar ciente ao utilizar nosso website.

Nós utilizamos medidas de segurança apropriadas para proteger seus dados pessoais, mas devido ao atual estado de desenvolvimento tecnológico, não podemos garantir segurança total, irrestrita e 100% absoluta para seus dados pessoais. Fazemos de tudo que está ao nosso alcance, no entanto, para garantir a segurança da informação e utilização de meios tecnológicos, procedimentais e melhores práticas adequadas para a proteção de seus dados pessoais, frente a invasões maliciosas de terceiros ou eventual acesso indevido aos nossos servidores e práticas indevidas similares.

Nós poderemos modificar a presente Política de tempos em tempos.

3. COMO UTILIZAMOS COOKIES E TAGS?

"Cookies" são identificadores que são transferidos para o seu navegador ou dispositivo, que nos informam como e quando as páginas e recursos em nosso website são visitados, quantas pessoas as acessam e algumas informações sobre seus dispositivos.

“Tag” é uma denominação genérica para trechos de códigos que permitem a coleta de dados de usuários de um website, possibilitam a implementação de funcionalidades (p. ex. vídeos, imagens, etc), e permitem a utilização de cookies.

Quando um usuário visita nossos websites, são inseridos “cookies” no seu navegador (p. ex. Firefox, Internet Explorer, Chrome, etc) que realizam a coleta automática de determinados dados pessoais para que possamos (i) operacionalizar nosso website (cookies estritamente necessários) e (ii) obter informações agregadas sobre nossos usuários. Nossos websites também possuem (iii) eventuais cookies de terceiros que são utilizados para publicidade (cookies de publicidade/advertising).

Eis, abaixo, um resumo dos cookies utilizados pela **FERRANTE ADVOGADOS** em nosso website:

- **Cookies essenciais**: Para acesso a áreas específicas do website da **FERRANTE ADVOGADOS**, permitindo a navegação do website e utilizações de suas aplicações, tal como acesso a áreas seguras por meio de login, sem os quais os serviços não podem ser prestados).
- **Cookies analíticos:** Para analisar a forma como os usuários usam o site e monitorar a performance deste. Por exemplo, para saber as páginas mais populares, qual o método de ligação entre páginas que é mais eficaz, ou para determinar a razão de algumas páginas receberem mensagens de erro.
- **Cookies de funcionalidade**: para permitir relembrar as preferências do usuário e oferecer funcionalidade para fornecer serviços avançados ao usuário. Em resumo, os cookies de funcionalidade guardam as preferências do usuário relativamente à utilização do site, de forma que não seja necessário voltar a configurar o site cada vez que o visita.
- **Cookies permanentes**: Ficam armazenados ao nível do navegador de internet (browser) nos dispositivos de acesso (pc, mobile e tablet) e são utilizados sempre que o usuário faz uma nova visita ao site. Geralmente são utilizados para direcionar a navegação de acordo com os interesses do usuário, permitindo a **FERRANTE ADVOGADOS** prestar um serviço mais personalizado.
- **Cookies de sessão** – São temporários, permanecem nos cookies do navegador de internet (browser) até sair do site. A informação obtida permite identificar problemas e fornecer uma melhor experiência de navegação.
- **Cookies de publicidade –** Para direcionar a publicidade em função dos interesses de cada usuário e do número de visitas que realizou, permitindo limitar o número de vezes da exibição do anúncio. Estes cookies ajudam a medir a eficácia da publicidade.

O visitante de nosso website pode optar por recusar ou desabilitar os Cookies por meio das configurações do seu navegador, ou ao instalar um plug-in que realize essa funcionalidade. No entanto, ao fazer isso, algumas áreas de nossos websites podem não funcionar corretamente. Ainda, esta Política não cobre o uso de cookies por terceiros, e não somos responsáveis por suas políticas e práticas de privacidade.

3. COM QUEM A FERRANTE ADVOGADOS COMPARTILHA OS DADOS PESSOAIS COLETADOS?

A **FERRANTE ADVOGADOS** poderá operar em conjunto com outras empresas ou parceiros comerciais numa ampla gama de atividades, principalmente no uso de serviços auxiliares ao funcionamento dos websites e para obtenção de informações sobre os usuários. Dessa forma, nos reservamos no direito de compartilhar suas informações com as empresas e/ou pessoas principalmente abaixo indicadas e, sempre que for possível, o faremos de forma anonimizada. Nós não emprestamos ou vendemos seus dados pessoais para ninguém. Nós podemos

compartilhar seus dados pessoais com as empresas mencionadas abaixo, de acordo com as finalidades (descrição de serviço) mencionadas abaixo.

A **FERRANTE ADVOGADOS** pode compartilhar todas as informações que coleta sobre os Usuários do website com parceiros e/ou contratados do **FERRANTE ADVOGADOS**, que são contratados exclusivamente para poder oferecer os Serviços contidos nos websites, ou para personalizar e/ou customizar sua experiência de usuário, ou, ainda, para o quanto previsto ao longo da presente Política.

Nossos parceiros somente são autorizados a utilizar os dados pessoais para os fins específicos que eles foram contratados, conforme abaixo, e, portanto, eles não irão utilizar os seus dados pessoais para outras finalidades, além as da prestação dos serviços previstos contratualmente e do quanto aqui previsto. Os atuais parceiros com quem compartilhamos os seus dados são:

Parceiros	Descrição do serviço
Google Analytics (https://analytics.google.com/) e Hotjar (https://www.hotjar.com/).	**Obter informações estatísticas sobre o uso dos nossos websites.**
Pagseguro, Asaas, PICPAY, e soluções financeiras similares	**Efetuar pagamento seguro na compra de produtos do website, oferecidos pela FERRANTE ADVOGADOS**
Correios	**Envio de correspondências físicas da FERRANTE ADVOGADOS quando necessário**
Facebook, Whatsapp, Telegram, Youtube, Instagram, Linkedin, Twitter, Tiktok, e redes sociais similares,	**Personalizar a experiência de navegação do usuário, mediante ferramentas de análise de experiência de dados, conforme políticas de dados pessoais de cada umas destas empresas**
Go Daddy	**Serviço de armazenagem de websites e arquivos do escritório**
Onedrive	**Serviço de armazenagem de arquivos do escritório**
Zoom Meetings, Google meets, Teams e similares	**Serviços de reunião online**

Para resguardar e proteger direitos da **FERRANTE ADVOGADOS**, a **FERRANTE ADVOGADOS** se reserva no direito de acessar, ler, preservar e fornecer quaisquer dados e informações sobre os

Usuários, incluindo interações suas, caso sejam necessários para cumprir uma obrigação legal ou uma ordem judicial; para fazer cumprir ou aplicar outros acordos e/ou contratos; ou proteger os direitos, propriedade ou segurança da FERRANTE ADVOGADOS, bem como de nossos funcionários e/ou outros Usuários.

ANEXO I – INFORMAÇÕES ADICIONAIS

1. COM QUEM CONTROLADOR COMPARTILHA OS SEUS DADOS?

O CONTROLADOR não compartilha os dados pessoais com terceiros, exceto aqueles relacionado à garantir a segurança da informação do CONTROLADOR, para o gerenciamento das atividades da FERRANTE ADVOGADOS, incluindo parceiros relacionados a eventuais cobranças e/ou serviços terceirizados para a atividade-fim da FERRANTE ADVOGADOS/CONTROLADOR, quando aplicável.

1. POR QUANTO TEMPO OS DADOS SERÃO ARMAZENADOS?

Nós manteremos os dados pessoais obtidos somente pelo tempo que for necessário para cumprir com as finalidades para as quais os coletamos, inclusive para fins de cumprimento de quaisquer obrigações legais, contratuais, de prestação de contas ou requisição de autoridades competentes.

Todos os dados coletados serão excluídos de nossas bases de dados quando o titular assim requisitar ou quando estes não forem mais necessários ou relevantes para as finalidades para os quais foram captados, salvo se houver qualquer outra razão para a sua manutenção, como eventual obrigação legal de retenção de dados, ou necessidade de preservação destes para resguardo de direitos do CONTROLADOR.

Para determinar o período de retenção adequado para os dados pessoais, consideramos a quantidade, a natureza e a sensibilidade dos dados pessoais, o risco potencial de danos decorrentes do uso não autorizado ou da divulgação de seus dados pessoais, a finalidade de processamento dos seus dados pessoais e se podemos alcançar tais propósitos através de outros meios, e os requisitos legais aplicáveis.

2. COMO FUNCIONA A SEGURANÇA DA INFORMAÇÃO NO CONTROLADOR.

O CONTROLADOR toma todas as providências técnicas e organizacionais para proteger os dados pessoais dos titulares contra perda, uso não autorizado ou outros abusos. Os dados serão armazenados em um ambiente operacional seguro que não é acessível ao público.

Nós nos esforçamos para proteger a privacidade dos dados pessoais que armazenamos, mas infelizmente não podemos garantir total segurança. O uso não autorizado de contas, falha de hardware ou software e outros fatores podem comprometer a segurança dos seus dados pessoais a qualquer momento, por isso, nos ajude a manter um ambiente seguro para todos. Além de adotar boas práticas de segurança em relação a seus dados pessoais, caso o Usuário identifique ou tome conhecimento de algo que comprometa a segurança dos dados pessoais, por favor entre em contato conosco por meio do e-mail a seguir: **douglasferrante@ferranteadvogados.com**

3. TRANSFERÊNCIA INTERNACIONAL

O CONTROLADOR não transfere diretamente dados pessoais coletados no Brasil para outros países, via de regra, podendo, não obstante, por decorrência de eventual software e/ou

aplicativo interno que venha a utilizar, para a prestação de seus serviços e/ou gerenciamento de seus serviços e/ou soluções de segurança, softwares e/ou programas e/ou apps para os quais haja uma necessária transferência de dados internacional apenas e tão somente para fins de operabilidade do software, programa e/ou solução de segurança. Consulte o DPO do CONTROLADOR caso queira ter mais informações sobre o tema.

4. COMO FALAR COM O ENCARREGADO DE DADOS DO CONTROLADOR?

Se você acredita que suas informações pessoais foram usadas de maneira incompatível com esta Política ou com as suas escolhas enquanto titular destes dados, ou, ainda, se você tiver outras dúvidas, comentários ou sugestões relacionadas a esta Política, você pode entrar em contato com nosso time nos seguintes endereços de contato:

Email: **douglasferrante@ferranteadvogados.com**

5. ATUALIZAÇÕES DESTA POLÍTICA

Como estamos sempre buscando melhorar nossos serviços, esta Política pode passar por atualizações, visando oferecer ao titular mais segurança, conveniência e melhorar cada vez mais a sua experiência. É por isso que recomendamos que o titular acesse nossa Política periodicamente, para que tenha conhecimento sobre as modificações.

6. INFORMAÇÕES ADICIONAIS

Informações adicionais e como respeitamos todos os direitos relacionados à proteção de dados pessoais de acordo com a LGPD:

Todas as atividades do CONTROLADOR relacionadas a dados pessoais obedecem a todos os fundamentos da LGPD, que são:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Além disso, também atuamos, em todas as nossas atividades envolvendo dados pessoais, nos pautando de acordo com os seguintes princípios da LGPD:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, 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.

Os fundamentos que utilizamos para o tratamento dos seus dados pessoais, como explicamos acima, são, via de regra, baseadas em consentimento, conforme explicamos acima, sendo que este é apenas um dos meios possíveis para o tratamento dos dados pessoais, que, de acordo com a LGPD, podem ser os seguintes:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

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 o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Quanto ao tratamento de dados pessoais cujo acesso é público, caso isso ocorra, O CONTROLADOR garante obedecer ao quanto disposto na presente Política, e agir de acordo com a LGPD, sendo certo que O CONTROLADOR obedecerá a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. Será dispensada a exigência do consentimento mencionado para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na LGPD.

Nos casos em que obtivermos o seu consentimento para tratamento dos seus dados pessoais, nos termos do quanto descrito nessa Política, e caso seja necessitário comunicar ou compartilhar dados pessoais com outras FERRANTE ADVOGADOSs, garantimos que iremos obter consentimento específico seu (Titular) para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas na LGPD. A eventual dispensa da exigência do consentimento não desobriga O CONTROLADOR das demais obrigações previstas na LGPD, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Além disso, o tratamento posterior dos dados pessoais relativos aos dados pessoais públicos, seja necessário para novas finalidades, observarão os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na LGPD.

Em nenhuma hipótese faremos o tratamento de seus dados pessoais mediante vício de consentimento.

Perceba que o seu consentimento, conforme é explicado nessa Política, se relaciona com finalidades bem determinadas, conforme já foi explicado acima, principalmente nos quadros explicando a finalidade de cada dado pessoal obtido, sendo certo que não utilizamos autorizações genéricas para o tratamento de dados pessoais, pois ela são nulas, de acordo com a LGPD, e nosso compromisso é respeitar totalmente os seus direitos e manter você sempre informado e inteirado sobre seus dados pessoais, dando a você total controle sobre eles, e, mais do que isso, confiança em sua relação com O CONTROLADOR.

O seu consentimento pode ser revogado a qualquer momento mediante a sua manifestação expressa, bastando que você envie um e-mail para: **douglasferrante@ferranteadvogados.com** São ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

Abaixo, apresentamos uma lista dos seus principais direitos. Em caso de alteração de informação referida nos itens I, II, III ou V abaixo, fique tranquilo: O CONTROLADOR te informará, com destaque de forma específica do teor das alterações, e você poderá, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração. Vamos aos seus principais direitos, de acordo com a LGPD:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação dO CONTROLADOR;

IV - informações de contato dO CONTROLADOR;

V - informações acerca do uso compartilhado de dados dO CONTROLADOR e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento de seus dados pessoais; e

VII - confirmação da existência de tratamento;

VIII - acesso aos dados pessoais;

IX - correção de dados incompletos, inexatos ou desatualizados;

XI - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;

XII - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

XIII - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas na LGPD, que são as seguintes - os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: (i) cumprimento de obrigação legal ou regulatória pelO CONTROLADOR; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou (iv) uso exclusivo dO CONTROLADOR, vedado seu acesso por terceiro, e desde que anonimizados os dados.

XIV- informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

XV - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

XVI - revogação do consentimento

XVII – término do tratamento de dados pessoais, que ocorre nas seguintes hipóteses: (i) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) fim do período de tratamento; (iii) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme já explicado acima, resguardado o interesse público; ou (iv) determinação da autoridade nacional de proteção de dados (ANPD), quando aplicável.

Perceba que todos esses direitos foram explicados ao longo dessa Política, mas fique à vontade para nos contatar no e-mail a seguir caso tenha ficado alguma dúvida: **douglasferrante@ferranteadvogados.com**

ANEXO II – POLÍTICA DE CÂMERAS DE SEGURANÇA

1. **Introdução:** A tecnologia das câmeras de segurança presentes do CONTROLADOR visam assegurar aos visitantes segurança em relação à sociedade brasileira que apresenta um elevado índice de crimes.
2. **Dados pessoais tratados:** As câmeras de segurança podem, por consequência, sujeitam eventuais pessoas que utilizam o espaço físico do CONTROLADOR ao tratamento de seus dados pessoais faciais/sua imagem e/ou
3. placa de veículo relacionados ao monitoramento efetuado pelas câmeras de segurança.
4. **Finalidades do tratamento:** É possível que imagens ou gravações de vídeo sejam feitas de você. Usamos tecnologia de vídeo-vigilância, principalmente, nas entradas de nossas instalações e em pontos críticos de segurança. Em qualquer caso, as câmeras são montadas de forma visível e identificadas. Essas câmeras ajudam a reduzir o risco de acesso não autorizado às instalações, tranquilizar os clientes e visitantes e fornecer um registro preciso do que aconteceu quando um incidente ocorre. A fim de proteger seus negócios, funcionários, clientes e outras partes interessadas, o CONTROLADOR faz uso do CCTV (Circuito Fechado de Televisão (closed-circuit television – CCTV – ou, em outras palavras, câmeras de segurança) em circunstâncias apropriadas para abordar áreas especificas de risco – inclusive estacionamento. Ao coletar e usar esses dados de vídeos (e possivelmente de áudio) o CONTROLADOR está sujeito a uma variedade de leis, incluindo a Lei Geral de Proteção de Dados (LGPD), que controla como tais atividades podem ser realizadas e as proteções que devem ser postas em prática para proteger as informações registradas.
5. **Segurança de dados e informações:** As imagens gravadas são protegidas de maneira que levam em conta o nível de risco e a sensibilidade das informações contidas. Quando apropriado, técnicas de criptografia podem ser usadas para garantir a confidencialidade em situações como o roubo do equipamento de gravação. Se o armazenamento em nuvem é usado, a devida diligência é realizada para garantir que o nível de proteção dos dados seja adequado. No caso de gravações do CCTV que precisem ser usadas como parte de um processo legal, são tomadas as devidas precauções para garantir que as imagens permaneçam aceitáveis no processo.
6. **Acesso aos dados de segurança:** Sob a LGPD, o indivíduo titular dos dados pode enviar uma solicitação de acesso para obter imagens do CCTV nas quais ele apareça, para o DPO - **douglasferrante@ferranteadvogados.com**
   Tais solicitações estão sujeitas aos procedimentos do CONTROLADOR, que inclui todas as verificações necessárias para averiguar o direito legal de acesso e a identidade do solicitante. Quando aprovado, as imagens gravadas podem ser visualizadas (sujeitas a controles de acesso) ou um registro das imagens pode ser fornecido.
   Solicitações para divulgar imagens do CCTV devem ser aprovadas pelo DPO em todos os casos. A divulgação não autorizada de imagens do CCTV (incluindo a publicação na Internet e na mídia) resultará na tomada de medidas disciplinares. Quando apropriado, ações são ser tomadas para ofuscar a identidade das pessoas e informações que não são relevantes para a solicitação.
7. **Período de retenção:** 7 dias ou conforme necessário para fins de segurança.

ANEXO III - POLÍTICA DE RECURSOS HUMANOS RELACIONADA À PROTEÇÃO DE DADOS PESSOAIS

1. INTRODUÇÃO

A presente política tem por objeto regulamentar a política de recursos humanos relacionadas à proteção de dados pessoais do CONTROLADOR, seja os recursos humanos exercido por terceiros, como é feito atualmente, seja na hipótese futura ou intermitente de vir a ser exercido pelo próprio CONTROLADOR.

A presente seção trata de conceitos-chave mencionados ao longo deste Guia. Para melhor disposição, os termos foram agrupados de acordo com: (i) conceitos gerais sobre a LGPD e sobre temas de Recursos Humanos; (ii) conceitos específicos sobre princípios previstos na LGPD; (iii) e conceitos específicos sobre direitos do(a)s titulares consoante a LGPD. Todas as definições foram dispostas por ordem alfabética.

2. CONCEITOS

2.1. CONCEITOS GERAIS

AGENTE DE TRATAMENTO: o controlador e o operador (Art. 5º, IX, LGPD).

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 (Art. 5º, XI, LGPD). O dado anonimizado, nos termos da lei, deixa de ser considerado dado pessoal, garantindo maior liberdade no seu tratamento (Art. 12, LGPD).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS (“ANPD”): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo território nacional (Art. 5º, XIX, LGPD). A ANPD foi instituída pela LGPD como órgão da administração pública federal com autonomia técnica, integrante da Presidência da República, definida sua natureza como transitória e passível de transformação pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República (Art. 55-A).

BASE LEGAL: trata-se do fundamento que autoriza o tratamento de dados pessoais por um agente, devendo ser definida, em casos concretos, a partir de uma das hipóteses dispostas na LGPD ao seu artigo 7º (caso de dados pessoais) ou ao seu artigo 11 (caso de dados pessoais sensíveis). As bases legais só não serão necessárias nos casos em que a LGPD não se aplica, como nas hipóteses do artigo 4º ou em situações de processamento que envolvam dados anonimizados, onde a identificação da titularidade não seja possível por meios razoáveis.

CONSENTIMENTO: manifestação livre, informada e inequívoca (Art. 7º, I, LGPD) pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Art. 5º, XII, LGPD). Deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (Art. 8º, LGPD).

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Art. 5º, VI, LGPD). É quem determina como os dados são processados

CRIANÇA: pessoa até doze anos de idade incompletos (Art. 2º do ECA).

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável (Art. 5º, I, LGPD). Também são considerados dados pessoais para os fins da lei aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (Art. 12, §2º, LGPD).

DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Art. 5º, II, LGPD).

ENCARREGADO (DATA PROTECTION OFFICER - "DPO"): é a pessoa física ou jurídica indicada pelo Agente de Tratamento para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

GDPR (GENERAL DATA PROTECTION REGULATION): Regulamento Geral sobre a Proteção de Dados 2016/679. Trata-se de regras relativas à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Revogou a Diretiva 95/46 /CE (Regulamento Geral de Proteção de Dados).

LGPD (LEI GERAL DE PROTEÇÃO DE DADOS): Lei 13.709/2018 dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (Art. 1º, LGPD). Aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: (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 (Art. 3º, caput e incisos I a III, LGPD).

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Art. 5º, VII, LGPD). É quem acata as ordens de como os dados devem ser processados.

ÓRGÃO DE PESQUISA: é o órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional, em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (Art. 5º, XVIII, da LGPD)

ÓRGÃO/DEPARTAMENTO/UNIDADE DE RH: todo órgão, departamento ou unidade que desempenha, mesmo que secundariamente, função de gestão de RH, ainda que de maneira secundária ou episódica. Essa função é verificada no exercício das tarefas relacionadas à seleção, contratação, pagamento, acompanhamento durante a vigência da prestação de serviço, e desligamento de funcionários/ associados/ colaboradores.

TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (Art. 5º, V, LGPD)

TRATAMENTO: 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 (Art. 5º, X, LGPD).

TRANSFERÊNCIA INTERNACIONAL DE DADOS: é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (Art. 5º, XV, LGPD).

UNIÃO EUROPEIA ("UE"): é um bloco econômico composto por 28 países da Europa (27 com o Brexit, isto é, com a saída do Reino Unido), sendo eles: Áustria, Bélgica, Bulgária, Croácia, Chipre, República Checa, Dinamarca, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Holanda, Polônia, Portugal, Romênia, Eslováquia, Eslovênia, Espanha, Suécia, Reino Unido

2.2. PRINCÍPIOS DA LGPD

Na terminologia jurídica, um princípio é um tipo de norma que deve ser cumprida na maior medida possível e cujo conteúdo serve como diretriz geral de interpretação para situações concretas. Na LGPD, os princípios estão listados ao longo do artigo 6° e são os seguintes:

ADEQUAÇÃO: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (art. 6º, II, LGPD).

BOA-FÉ: significa a observância de um comportamento leal, correto e probo na realização das atividades de tratamento de dados pessoais. Esse princípio, opera como norte a todos os demais e servindo de baliza para interpretar conceitos abertos (art. 6º, caput, LGPD).

FINALIDADE: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível ou desvirtuada (art. 6º, I, LGPD).

LIVRE ACESSO: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6º, IV, LGPD).

NÃO DISCRIMINÇÃO: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (art. 6º, IX, LGPD).

NECESSIDADE: limitação ou minimização do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (art. 6º, III, LGPD).

PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII, LGPD).

QUALIDADE DOS DADOS: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (art. 6º, V, LGPD).

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS: demonstração, pelo agente, 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 (art. 6º, X, LGPD).

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 (art. 6º, VII, LGPD).

TRANSPARÊNCIA: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI, LGPD).

2.3. DIREITOS DO TITULAR NA LGPD

Os direitos dos titulares de dados estão previstos majoritariamente ao longo do artigo 18 da LGPD. Ademais, há ainda o direito de titularidade (artigo 17) e, com relação a tratamentos automatizados, os direitos de informação e de revisão (artigo 20):

ACESSO AOS DADOS: o titular de dados tem resguardado o seu interesse de receber uma cópia dos dados pessoais detidos pela empresa, se assim o requisitar (art. 18, II, LGPD). Conforme a LGPD, tal direito será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências (art. 13, § 3º, LGPD). Sublinha-se que os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as suas finalidades (art. 23, § 5º, LGPD).

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO: o titular de dados tem o direito de solicitar que seus dados sejam anonimizados, bloqueados ou que haja a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei (art. 18, IV, LGPD).

CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO: direito do titular a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição de informações sobre a existência de tratamento (art. 18, I, LGPD), isto é, de toda operação realizada com seus dados pessoais (art. 5º, X, LGPD).

CORREÇÃO DE DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS: o titular de dados pode requerer a retificação dos dados, caso estejam incorretos, insuficientes, imprecisos, não expressem a completude das informações armazenadas ou careçam de atualização (art. 18, III, LGPD).

ELIMINAÇÃO DOS DADOS PESSOAIS: o titular de dados pode requerer que seus dados sejam excluídos, de forma que a empresa deverá eliminar todos os dados coletados com relação a esse titular, a não ser que exista outra base legal para a manutenção desses dados (art. 18, VI, LGPD).

INFORMAÇÃO SOBRE COMPARTILHAMENTO: o titular de dados pode solicitar informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII, LGPD).

INFORMAÇÃO SOBRE O NÃO CONSENTIMENTO: o titular de dados pode solicitar informações sobre a possibilidade e hipóteses de não fornecimento do consentimento, além de entender sobre as consequências da negativa (art. 18, VIII, LGPD).

INFORMAÇÃO SOBRE TRATAMENTO AUTOMATIZADO: o titular de dados pode pedir informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. Tais informações, a serem oferecidas pelo controlador, deverão apresentar clareza e adequação com o que foi solicitado (art. 20, §1º, LGPD).

OPOSIÇÃO: o titular de dados pode se opor ao contexto do tratamento de dados e/ou às finalidades do tratamento, incluindo tratamento realizado com fundamento em uma das hipóteses de dispensa do consentimento (art. 18, §2º, LGPD).

PETIÇÃO: o titular de dados pode fazer qualquer requerimento com relação aos seus dados contra o controlador perante a autoridade nacional (art. 18, §1º, LGPD).

PORTABILIDADE: disponibilização dos dados do titular a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador (art. 18, V, LGPD).

REVISÃO: o titular de dados pode pedir revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20, caput, LGPD).

REVOGAÇÃO DO CONSENTIMENTO: manifestação expressa do titular, por procedimento gratuito e facilitado (art. 18, IX, LGPD), ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (art. 8º, §5º, LGPD).

TITULARIDADE DOS DADOS PESSOAIS: a toda pessoa natural é assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade (art. 17, LGPD), de modo que o titular é, portanto, a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V, LGPD).

3. ESCOPO DE APLICAÇÃO

Este Guia, juntamente com os demais materiais elaborados no âmbito do Programa de Conformidade do CONTROLADOR para com a LGPD, serve de base para que todos os colaboradores contratados diretamente ou terceirizados que realizem a função de RH, ainda que de maneira secundária ou esporádica, possam: (i) verificar se os procedimentos já instaurados, que envolvam operações de tratamento de dados pessoais, estão sendo feitos da maneira apropriada, de acordo com a LGPD; (ii) orientar-se sobre como proceder diante de novas operações de tratamento de dados pessoais que surjam em sua atividade

4.OBJETIVOS

São objetivos do Guia de Proteção de Dados: Recursos Humanos:

(a) Estabelecer, de forma geral, as principais responsabilidades do CONTROLADOR no que diz respeito às rotinas de gestão de recursos humanos que envolvam tratamento de dados pessoais, apontando diretrizes que assegurem e reforcem o compromisso do CONTROLADOR com as práticas previstas na LGPD;

(b) Descrever as regras comportamentais a serem seguidas na condução das atividades desenvolvidas no CONTROLADOR, inclusive no que tange a seus aspectos de recursos humanos, próprio ou terceirizado, que garantam a conformidade com a LGPD, especialmente no atinente à atividade de gestão de RH; e

(c) Abordar atividades de gestão de RH que devem ser reguladas em razão da alteração legislativa;

5. POR QUE É RELEVANTE A PROTEÇÃO DE DADOS RELACIONADA A RECURSOS HUMANOS?

As áreas de Recursos Humanos são responsáveis pelo tratamento de uma série de dados pessoais de diferentes tipos de colaboradores próprios ou terceirizados. Isso porque essa área lida com informações identificadas dos colaboradores, como RG, CPF e e-mail, bem como com dados que, quando agregados, cruzados ou enriquecidos, podem tornar uma pessoa identificável. Por exemplo: IP (internet protocol), cookies, histórico de navegação, cursor do mouse etc. O restante deste documento se divide em 4 tópicos específicos sobre a área de RH, sendo o primeiro (seções 5.1 e 5.2) elaborado para aprofundar a temática de a quem este Guia se destina, bem como para esclarecer como as legislações já existentes que regulam atividades da área de RH se relacionam com a LGPD; o segundo (seção 6) indica como devem ser tratados os dados pessoais de candidatos(as) a colaborador(a); o terceiro (seção 7) destinado a esclarecer como devem ser tratados os dados daqueles colaboradores efetivados; e o quarto (seção 8) destinado a identificar como deve ser o tratamento dos dados pessoais dos colaboradores após seu desligamento.

5.1. A QUEM SE DESTINA ESTE GUIA? QUEM SE ENQUADRA COMO “RECURSOS HUMANOS”?

Em todos os casos nos quais há um vínculo entre um colaborador e o CONTROLADOR, diretamente ou indiretamente (terceirizado), em geral há um órgão ou área interna responsável pela regularização e administração deste vínculo, a área de gestão de Recursos Humanos (Unidade de RH). O setor de recursos humanos pode trabalhar com diferentes regimes de colaboração, sejam vínculos de emprego, de prestação de serviço ou outros tipos, representados, ilustrativamente, conforme melhor explicitado abaixo. Essas colaborações, note-se, nem sempre são gerenciadas por um único órgão dentro de uma pessoa jurídica ou condomínio, podendo variar a depender do tipo de vínculo gerado ou do tipo de rotina realizada. Por exemplo, a seleção de pessoal pode, em determinados casos, ser feita pela administradora do CONTROLADOR, como é o caso atualmente. As orientações deste Guia se aplicam às situações em que o vínculo entre colaboradores e CONTROLADOR são constituídos e administrados por uma área dedicada, a Unidade de RH, seja própria ou terceirizada, bem como às situações em que o são por áreas cuja ocupação principal não é a gestão de Recursos Humanos. Em suma, se aplicam a todos os colaboradores que desempenham, de modo principal ou não, qualquer função de gestão de Recursos Humanos com algum tipo de relação ao CONTROLADOR, seja diretamente ou indiretamente (como no caso da administradora do CONTROLADOR).

5.2. RELAÇÃO COM OUTRAS FONTES REGULATÓRIAS E O CONCEITO DA OBRIGAÇÃO LEGAL

Como visto logo na seção anterior, existem diferentes formas de vinculação de colaboradores ao CONTROLADOR, seja diretamente ou indiretamente. Todas estas formas são de responsabilidade de alguma área que, ainda que não seja designada como “Unidade de RH”, assume a função de gestão de RH. O cuidado com o tratamento de dados pessoais, no entanto, não é uma novidade para essas unidades. Isso porque existe uma ampla gama de leis e regulamentações trabalhistas que, por si só, já determinavam obrigações que implicavam uso de dados pessoais ou, no dizer da nova Lei, implicavam tratamento de dados pessoais. Nesse sentido, é importante verificar como a LGPD se relaciona com estas regulações preexistentes, já cumpridas pela Unidade de RH, no que tange especificamente ao tratamento de dados pessoais.

De modo geral, a recomendação dada consiste em sempre realizar o tratamento de acordo com a lei ou regulamentação aplicável. Isso porque a própria LGPD estipula que o tratamento de dados pessoais é autorizado quando feito para cumprir com obrigação legal ou regulamentar existente (Art. 7, II, da LGPD).

Atenção: A LGPD não substitui nem impede o tratamento de dados realizado em conformidade com outras leis ou regulamentos.

Caso as normas que regulem o vínculo aqui discutido e que versem sobre o tratamento e armazenamento de algum dado pessoal sejam vagas quanto aos ciclos de vida, por exemplo, ou sobre formas de armazenamento e de eliminação, deve-se guiar pelos princípios e diretrizes da LGPD, que serão apresentadas nesse Guia.

Dentre os regulamentos existentes, importante fazer especial menção àqueles que mais afetam o CONTROLADOR em sua área interna ou terceirizada de gestão de Recursos Humanos. Nesse sentido:

(i) Legislação trabalhista. Devem ser tratados os dados pessoais de acordo com a lei trabalhista, quando for o caso. Nesse sentido, indica-se que quanto aos documentos para admissão e desligamento de colaboradores será explicado em tópico seguinte.

(ii) Eventuais legislações setoriais que atualmente ou futuramente lidem com o tema. Nesses casos, esta continua vigendo de acordo com suas disposições sobre o tempo de descarte e eliminação do dado pessoal coletado. Isso porque nesse caso já existiria uma fonte legislativa que justifica a necessidade do tratamento de dados e que já condiciona esse tratamento a um período específico.

(iv) Demais casos. Na hipótese de o tratamento do dado ser autorizado por uma lei trabalhista, mas o seu armazenamento não estar condicionado a um prazo específico, será utilizado um critério de razoabilidade para sua manutenção.

Nessas hipóteses, o procedimento de ciclo de vida tem de ser avaliado caso a caso, identificando a justificativa para a coleta e preservação do dado:

(i) Em regra, recomenda-se que os dados sejam preservados pelo prazo de guarda necessário para fazer frente a eventuais demandas judiciais, trabalhistas ou não, de acordo com a forma de vinculação. (ii) Superado o prazo de guarda, os dados devem ser eliminados, tanto aqueles que estejam em forma física como os que estejam em forma digital. (iii) Outras justificativas devem ser analisadas caso a caso, devendo ser formulada consulta ao Encarregado (DPO) para que ele avalie se é legalmente correto preservar ou não o dado. (iv) Deve-se ter especial cuidado com os dados sensíveis (como um atestado que indique se existe doença do trabalho ou não), pois a sua manutenção indevida gera altos riscos para o titular de dados pessoais e para a pessoa jurídica contratante ou ofertante da vaga. A seguir, exemplos de documentos e dados pessoais sensíveis ou não:

CURRÍCULOS	CONTÉM DADOS SENSÍVEIS?
Dados pessoais como: CPF, RG e dados da conta bancário usados para o cadastro no	Não

sistema da base de dados dos funcionários/associados	
Dados médicos obtidos em exame admissional	Sim
Dados de funcionários e seus familiares coletados para o seguro de saúde, quando existente	Sim

Essas hipóteses acima são meramente exemplificativas. Pode haver exceções às regras, como nos casos de currículos de pessoas com deficiência em que a condição seja declarada, onde existiriam, portanto, dados sensíveis.

Atenção: O dado pessoal só pode ser preservado enquanto houver justificativa, como, por exemplo, o prazo prescricional de uma ação trabalhista. Prazo prescricional significa o prazo em que o empregado ou ex-empregado podem ingressar com uma ação trabalhista. Esse prazo é estabelecido na CLT, via de regra, ou em lei especial, caso seja o caso de um cargo específico regulado por lei especial.

As justificativas para a coleta e armazenamento de dados pessoais são chamadas, juridicamente, de bases legais (Arts. 7º e 11, LGPD). Uma das principais bases legais que justificará o armazenamento de dados pessoais na atividade de gestão de RH será o cumprimento de obrigações legais e regulamentares. No entanto, existem outras bases previstas em lei, merecendo destaque para fins deste Guia: (i) o consentimento; o (ii) legitimo interesse; e a (iii) execução de contrato. Nas seções seguintes, indicamos os principais processos e rotinas desempenhados pela Unidade de RH que envolvem tratamento de dados pessoais, as bases legais para sua realização, e as principais recomendações para a adequação à LGPD.

6. LIDANDO COM DADOS NOS PROCESSOS SELETIVOS

Alguns vínculos entre colaboradores e CONTROLADOR, seja diretamente ou por terceirização, para serem efetivados, estão condicionados a um processo de seleção. A realização desse simples processo de seleção envolve uma série de tratamentos de dados pessoais do candidato interessado. Justamente por esse motivo, a seleção deve ser feita em observância à LGPD. Cumpre esclarecer que as recomendações aqui dispostas são aplicáveis tanto caso o colaborador seja admitido, bem como na hipótese de o candidato não ser admitido.

6.1. DADOS TRATADOS EM PROCESSO SELETIVO

Os tratamentos de dados pessoais (coleta, armazenamento, compartilhamento etc.) no processo de seleção têm de estar em conformidade com a LGPD. Fundamentalmente, isto significa que é necessário possuir: (i) uma base legal para realizar esse tratamento, (ii) uma finalidade bem definida quanto ao tratamento feito; (iii) a adequação entre o tratamento e a finalidade almejada. Para fins desse Guia, o tratamento dos dados pessoais em processo de seleção terá como base legal o consentimento do titular de dados. Isso porque, presume-se que o candidato, ciente das exigências para concorrer à vaga, bem como ciente dos dados que serão coletados, optou, de forma livre, por permitir que a área de RH trate seus dados. O consentimento do titular de dados pessoais consiste na manifestação livre, informada e

inequívoca pela qual o titular concorda com o tratamento dos dados pessoais para uma finalidade determinada. Cumpre detalhar brevemente as características do consentimento aqui indicadas. O consentimento de um titular de dados pessoais pode ser considerado como livre nas situações em que ele/ela expressa a sua escolha de forma espontânea e sem qualquer tipo de coerção ou coação. Importante notar, ainda, que o titular de dados deverá ser informado sobre a possibilidade do não fornecimento do consentimento e sobre as consequências da negativa. No caso do tratamento de dados para uma seleção, o candidato deverá ser informado, de forma clara e transparente, sobre quais dados pessoais deverão ser fornecidos por ele, sobre quais serão coletados independentemente do fornecimento do titular, e quais as consequências de não consentir com o fornecimento ou a coleta de tais dados (como a eliminação do processo seletivo, por exemplo). Ele será informado quando houver a indicação de informações claras, precisas, em linguagem acessível e de fácil compreensão. É elementar certificar que informações essenciais sobre a operação de tratamento, seus modos, os agentes envolvidos e os eventuais riscos não tenham sido omitidas do titular. Nesse sentido, ele terá mais controle com relação aos seus dados.

O adjetivo inequívoco, abrange o modo de manifestação, firme e claro, acerca da concordância do titular para o tratamento de seus dados. É imprescindível garantir que a pessoa natural concordou com as operações que serão realizadas com suas informações, de modo que o destaque das cláusulas de tratamento de dados pessoais deve ser sempre garantido ao titular de dados, seja em meio eletrônico ou impresso. Ou seja, sob a nova legislação de proteção de dados pessoais, além da confirmação clara do titular, este deve ter decidido sem quaisquer ambiguidades, confusões ou elementos que possam prejudicar a sua decisão.

ATENÇÃO! O consentimento deve sempre se referir a finalidades determinadas! As autorizações genéricas para o tratamento de dados pessoais serão nulas para fins de cumprimento da LGPD.

Explicada a noção de consentimento, é necessário ainda ressaltar que o seu conceito dificilmente poderá ser valorado isoladamente, de forma estática. O consentimento só pode ser considerado livre, informado e inequívoco se levada em conta a finalidade da operação de tratamento de dados pessoais. A finalidade é muito mais do que um mero acessório do consentimento, é um dos princípios da Lei Geral de Proteção de Dados Pessoais. Por finalidade, entende-se o propósito informado à pessoa natural acerca das operações que serão realizadas para tratar os seus dados. A conjugação do consentimento com a finalidade faz com que seja possível assegurar que, primeiro, o agente responsável pelo tratamento de dados pessoais tenha se esforçado para deixar claro quais os propósitos para a coleta, armazenamento e uso dos dados do titular e que, segundo, a anuência desse titular seja feita da forma mais esclarecida quanto for possível.

DICA: CONSENTIMENTO E FINALIDADE ANDAM JUNTOS: É necessário avaliar sempre qual o propósito do dado coletado: identifique a finalidade para qual este dado será usado. Em seguida, caso a base legal utilizada seja a do consentimento, avalie se ele está em sintonia para a finalidade estipulada. Finalidades distintas implicam consentimentos distintos.

Nesta seção, cuidaremos, exemplificativamente, das operações de tratamento mais comumente realizadas em processos seletivos.

(i) Coleta

- Quais dados posso coletar em processos seletivos?

Conforme exposto, para a realização da coleta é necessário que antes tenha-se determinado qual seria a sua finalidade. No caso da seleção de colaboradores, todos os dados pessoais coletados têm de estar diretamente relacionados ao processo seletivo, sendo estritamente necessários para que ele seja realizado. Nestes casos, existe uma clara finalidade em obter dados pessoais que revelem meios de identificar o candidato, bem como seu enquadramento à vaga pretendida. Razoável, portanto, coletar dados como: RG, CPF, e-mail, telefone de contato, pedido para que seja indicada a formação do candidato, experiência prévia na área etc. Há alguns tipos de dados, obtidos por meio de certidões, que merecem consideração especial, por existirem limitações à sua exigência em processos seletivos, especialmente decorrentes do Direito do Trabalho. A seguir elencaremos estas certidões e as orientações correspondentes. Cabe esclarecer que as orientações aqui fornecidas se referem ao sistema de proteção de dados pessoais trazido pela LGPD, apenas. No entanto, a justificativa do ponto de vista da proteção de dados depende de que a legislação específica aplicável ao processo seletivo permita a exigência de tais dados ou documentos. Assim, em todos os casos, as orientações adicionais cabíveis (sobre aspectos cíveis, trabalhistas etc.) deverão ser buscadas junto ao departamento jurídico ou prestador de serviço jurídico que presta assessoria em outros ramos de atuação do CONTROLADOR para além daquele relacionado à LGPD, de acordo com as leis específicas relacionadas aos aspectos cíveis, trabalhistas e correlatos.

- Certidão de distribuição de ações judiciais em que o candidato for parte

Poderia ser exigida do candidato uma certidão para verificar se existem ações judiciais em curso em que ele seja parte? Isso será respondido mais adiante. As ações aqui abrangem qualquer matéria, cível, criminal, trabalhista etc.

ATENÇÃO! As pesquisas conduzidas têm de estar vinculadas ao objeto da seleção.

- Certidão de antecedentes criminais

Poderia ser exigida do candidato a certidão negativa de antecedentes criminais? Isso será respondido mais adiante.

- Certidões emitidas por sistemas de proteção ao crédito (SPC, SERASA etc.)

Poderia ser exigida do candidato qualquer espécie de certidão obtida junto a órgãos de proteção ao crédito, como certidões de inexistência de dívidas ou de pontuação em sistemas de score de crédito? Isso será respondido abaixo.

Como regra geral, a resposta é negativa, nas três hipóteses elencadas acima. Contudo, pode haver exceções do ponto de vista da proteção de dados pessoais, nos casos em que a legislação aplicável ao processo seletivo (e.g. trabalhista) permita a exigência. Em geral, a legislação ou o judiciário têm permitido tal exigência nas situações em que as informações sobre a participação de candidato em ações judiciais, sobre seus antecedentes criminais ou sobre sua situação nos sistemas de proteção ao crédito sejam necessárias para julgar sua aptidão, principalmente em termos de confiabilidade, para a função que iria desempenhar. Seria o caso, por exemplo, de candidato que trabalhará em funções que envolvam movimentações financeiras, podendo-se

considerar mais confiável para tal função um candidato que não esteja sendo processado por dívidas, ou de candidato que trabalhará na área de segurança, caso em que é relevante saber se possui ação criminal em que seja réu para avaliar sua confiabilidade para a função. Dada a controvérsia em torno do tema e suas ramificações em outras áreas do Direito, além dos cuidados que a situação exige, na hipótese de se entender necessário exigir algum destes tipos de certidão, recomenda-se:

(i) Em primeiro lugar, deve ser consultado o departamento Jurídico que presta suporte à parte responsável pela contratação, de maneira devidamente documentada, para que informe se a exigência é permitida do ponto de vista da legislação trabalhista ou cível aplicável ao processo seletivo;

(ii) Em segundo lugar, deve ser consultado o Encarregado de proteção de dados responsável, para que sejam consideradas as questões de proteção de dados envolvidas.

Como recomendação mais geral, deve-se ponderar se as informações relativas a antecedentes criminais, penalidades administrativas, entre outras, são realmente imprescindíveis para a realização do processo seletivo. Isso porque a apresentação desses dados pode gerar uma situação de discriminação do candidato, e não se ater ao propósito de aferir a aptidão para a vaga pretendida. A presença de um antecedente criminal poderia significar o impedimento de participação no processo de seleção e, consequentemente, o impedimento do exercício da profissão, só devendo ser requerido quando necessário. Além disso, deve-se reiterar que a LGPD traz como um de seus princípios norteadores o da necessidade, estabelecendo uma limitação do tratamento de dados pessoais ao mínimo necessário para a realização das suas finalidades, devendo os dados serem pertinentes, proporcionais e não excessivos com relação às finalidades do tratamento.

- Posso coletar dados sensíveis?

Alguns processos seletivos podem ter como rotina solicitar algum dado pessoal que, nos termos da LGPD, seja considerado sensível. É o que ocorreria, por exemplo, em processos nos quais existisse uma cota específica de vagas destinadas à Pessoas Com Deficiência (PCD)[1]. Nesse caso, estariam sendo solicitados dados que podem sujeitar os titulares às situações de maior vulnerabilidade social. Por se tratar de informações que colocam os titulares de dados em situação de maior vulnerabilidade, o tratamento de dados pessoais sensíveis imputa maior responsabilidade aos que realizam o tratamento desses dados e exige maior atenção e cuidado em seu tratamento, objetivando alcançar um grau elevado de proteção. Formas possíveis para assegurar essa maior proteção consistem em tomar todas as providências possíveis para que: (i) um número restrito de pessoas tenha acesso às informações obtidas; (ii) esses dados fiquem em um servidor que assegure segurança e proteção às informações; e (iii) esses dados sejam, preferencialmente, criptografados. Da mesma forma, os dados pessoais sensíveis registrados em papel devem ser armazenados com cuidados especiais de segurança próprios desse formato.

[1] Segundo a Lei nº 13.146/2015 - Estatuto da Pessoa com Deficiência e a Convenção sobre os Direitos da Pessoa com Deficiência (promulgada em 2007) Art. 2º "Considera-se pessoa com deficiência aquela que tem impedimento de longo prazo de natureza física, mental, intelectual ou sensorial, o qual, em interação com uma ou mais barreiras, pode obstruir sua participação plena e efetiva na sociedade em igualdade de condições com as demais pessoas.". O enquadramento da condição de PCD como dado sensível, especificamente, baseia-se em considerar esta informação como um dado referente à saúde do titular.

É, portanto, possível coletar dados sensíveis, desde que se garanta mais proteção e segurança aos mesmos. A base legal para a coleta do dado sensível em um processo seletivo pode ser o consentimento, contanto que seja manifestado de forma específica e destacada, para finalidades específicas (Art. 11, I, LGPD), ou ainda o cumprimento de obrigação legal ou regulamentar (Art. 11, II, "a" da LGPD), caso haja regulamento ou lei específica que determine a sua coleta.

- Preciso de consentimento específico para coletar tais dados?

Na hipótese dos dados sensíveis requeridos forem, especificamente, relacionados à comprovação de que o candidato é PCD, não existe a necessidade do consentimento específico, visto que a fundamentação que justifica esse tratamento é a obrigação legal. Por exemplo, destaca-se que existe uma legislação especifica que prevê que as empresas possuam um percentual de vagas destinadas à PCD. No entanto, permanecem as obrigações de transparência quanto à coleta, armazenamento, eliminação e finalidade desses dados. Nos demais casos, assim como descrito na seção 6, a base utilizada para a coleta de dados em processos seletivos é a do consentimento. Também como demonstrado, nas hipóteses de coleta de dados sensíveis, é necessário maior cuidado, por serem dados que podem expor o titular à maior vulnerabilidade. Justamente em razão deste maior cuidado que se orienta que exista um consentimento específico na coleta e dados sensíveis para fins de processo seletivo. Existem dois modos de conseguir este consentimento específico. Nas hipóteses em que os dados forem coletados através do envio de documentos físicos ou digitalizados, deverá também ser preenchido um termo específico de consentimento sobre o tratamento dos dados pessoais, onde fique evidente a finalidade e o tratamento que será destinado para estes dados. Nas hipóteses em que os dados forem coletados via um meio eletrônico, deverá existir um campo em que possa ser marcado o consentimento. Sugere-se um campo em que possa marcar o consentimento sobre o tratamento dos dados pessoais, onde fique evidente a finalidade e o tratamento que será destinado para estes dados. O mesmo termo de consentimento pode ser adaptado para formato eletrônico.

ATENÇÃO!

A coleta dos dados pessoais e dados pessoais sensíveis está, necessariamente, condicionada ao consentimento específico do/da titular destes dados.

- O candidato pode dar consentimento parcial? Como proceder neste caso?

Existe a hipótese de o candidato concordar com o tratamento de alguns dados, mas não de todos. A Unidade de RH pode concordar com essa postura do candidato? Primeiramente, tem que se considerar que é uma opção de o candidato ceder ou não seus dados pessoais. Ele deve ser avisado, desde o início do processo seletivo, quais serão os dados pessoais necessários, bem como as consequências de estes não serem disponibilizados. Por exemplo, pode ser solicitado, em um edital ou chamada de contratação, que o candidato envie seu e-mail pessoal, para contato. Caso o candidato não queira ceder tal dado, ele deve ser informado que isso pode fazer com que ele não seja considerado para a vaga pretendida. De mesma maneira, o candidato deve ser informado que, caso ele não dê seu consentimento para a avaliação de determinadas

informações, estas não serão consideradas no processo avaliativo. Por exemplo, caso o candidato não informe sua etnia, ele não será considerado para as hipóteses de cotas. Ainda, caso ele não envie dados como sua carta de motivação, ou seu nome completo, ele não poderá sequer ser considerado para fins avaliativos. A partir do momento em que o candidato fornece estes dados, pode-se assumir que esta é uma manifestação do consentimento do titular e ele, portanto, consente com o tratamento destes (Art. 8º da LGPD). Ou disponibiliza ou torna público ele mesmo os seus dados, tais como em redes sociais (Linkedin).

(ii) Armazenamento

- Por quanto tempo os dados podem ser armazenados?

Não existe, nem na legislação trabalhista, nem na LGPD, uma previsão de lapso temporal específico para o armazenamento dos dados coletados em um processo seletivo. Por esse motivo se torna necessário fazer uma análise de prudência e razoabilidade. Primeiramente, é preciso avaliar qual a finalidade dos dados coletados. Em um processo seletivo, a finalidade é verificar se o candidato se adequa à vaga oferecida. Assim, o consentimento oferecido pelo candidato ao enviar a documentação solicitada em processo seletivo, se não houver previsão mais específica, será para o armazenamento dos dados pelo tempo necessário para a realização da seleção. Desse modo, a recomendação nas hipóteses de processos seletivos é que os dados devem ser excluídos assim que findo o processo de seleção.

ATENÇÃO! Dados pessoais sensíveis requerem maior atenção, também nas hipóteses de armazenamento. A coleta dos dados pessoais e dados pessoais sensíveis está, necessariamente, condicionada ao consentimento específico do titular destes dados.

- Os dados podem ser retidos por mais tempo, depois do processo de seleção?

Há a possibilidade de que, em um uma seleção, o candidato seja bem avaliado, mas não seja selecionado para a vaga disponível. Nesse caso, pode ser relevante para a pessoa jurídica que está realizando o processo seletivo manter os dados em sua base de dados caso surja uma nova oportunidade para chamar o candidato bem avaliado. Também existe a possibilidade de o próprio candidato ter interesse de ser chamado para outras vagas, mas em outra área ou órgão, ainda que tenha enviado o currículo apenas para seleção relativa a uma unidade específica. O candidato pode pretender, também, que seu e-mail continue na base de dados para que seja informado de novas vagas de emprego na unidade pretendida. Em ambas as hipóteses, os dados podem ser retidos por mais tempo do que o da seleção desde que o candidato tenha consentido de maneira específica com esses armazenamentos. Apenas caso haja consentimento, esse armazenamento poderá ser prolongado

6.2. DADOS ENVIADOS PELOS CANDIDATOS SEM SOLICITAÇÃO

Todos os dados pessoais exigidos no processo de admissão têm de estar estritamente relacionados com o objeto do recrutamento, com os quais os candidatos têm de ter consentido no início da seleção. No entanto, é certo que os candidatos podem, por vontade própria, enviar informações extras, não solicitadas pelos realizadores do processo de seleção. Nesse sentido,

como os próprios candidatos enviaram de livre e espontânea vontade tais dados, independentemente do pedido realizado, estes dados podem ser tratados para fins da seleção. Ressalta-se, nesse cenário, que o tratamento conferido a eles deve ser o mesmo dispensado aos dados solicitados, e devem ser usados para as mesmas finalidades.

ATENÇÃO! Os dados enviados sem solicitação não podem ser usados para finalidades diversas do que o processo seletivo.

Isso porque, de acordo com o Art. 8 da LGPD, o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Entende-se, então, que o candidato, ao enviar os dados a mais, consentiu com sua utilização no processo seletivo. Devem ser aplicados aos dados enviados sem solicitação os mesmos cuidados relativos aos dados pessoais solicitados. Há ainda uma outra situação em que ocorre o envio de dados não solicitados, que é o envio de currículos por iniciativa de interessados, quando não há processo seletivo aberto. Essa hipótese compreende o caso do interessado que envia currículo para que seja armazenado e considerado, caso venha a ser aberta alguma vaga disponível em que o seu perfil se encaixe. Também compreende currículos enviados mediante indicação de terceiros. Nestes casos, pode-se considerar que o candidato manifestou seu consentimento para que os dados enviados sejam considerados para o preenchimento de vagas eventualmente disponíveis, ou mesmo para vagas que venham surgir em um lapso de tempo razoável. Os dados poderiam, então, ser utilizados com tal finalidade. Fica a questão de se saber qual seria esse lapso de tempo razoável, tal que se possa considerar abrangido pelo consentimento do interessado no que diz respeito ao armazenamento dos dados enviados.

Entende-se que seria razoável manter o currículo do candidato por 1 (um) ano. Mais tempo não seria razoável, pois o currículo poderia estar desatualizado, o interesse na vaga poderia ter sumido, dentre outros fatores, que motivariam, por si só, uma nova seleção. Por esse motivo, se houver interesse em manter o currículo armazenado depois de decorrido um ano, recomenda-se que se busque junto ao candidato a renovação do consentimento.

- Dados pessoais sensíveis que foram enviados sem solicitação podem ser coletados?

O material enviado pelos candidatos que exceda o pretendido no edital ou chamada de seleção pode, eventualmente, conter dados sensíveis. Por exemplo, candidatos podem enviar uma amostra de material escrito (artigo, dissertação, tese), cartas de recomendação, comprovantes de certificação etc., que podem conter sua opinião política ou convicção religiosa, por exemplo. Nessas hipóteses, os dados podem ser coletados, já que se considerou que, no seu envio, foi manifestado o consentimento para sua utilização no processo seletivo em curso. Contudo, vale lembrar a orientação geral sobre os dados sensíveis, no sentido de conferir ao seu tratamento um nível maior de segurança. Assim, deve haver o cuidado para que um mínimo de pessoas tenha acesso aos dados sensíveis e que eles fiquem armazenados em locais que garantam sua segurança e proteção.

6.3. DADOS OBTIDOS POR OUTROS MEIOS

Além dos dados enviados pelos candidatos, em um processo seletivo há a possibilidade de coletar dados dos candidatos através de meios alternativos de pesquisa. Por exemplo, pode-se

ligar para o último empregador do candidato para verificar se ele possui as qualidades necessárias para a função pretendida.

De modo geral, essas pesquisas podem ser feitas desde que:

(i) A finalidade do uso de seus resultados esteja estritamente vinculada à realização do processo seletivo em curso.

(ii) O candidato seja informado de que tais pesquisas serão realizadas.

ATENÇÃO!

O responsável pelo processo seletivo deve estabelecer claramente quais são os dados pessoais relevantes para a candidatura da vaga, indicando tanto aqueles que devem ser fornecidos pelo candidato, como aqueles que poderão ser obtidos pelos recrutadores por outros meios (e.g. pesquisa no LinkedIn).

Nesta hipótese de pesquisa de dados pessoais dos candidatos feita diretamente pelo recrutador, três tipos de documentos que contêm dados pessoais, sobre os quais se comentou anteriormente ("Coleta"), voltam a ter importância e merecem considerações especiais. São eles:

(i) Certidão de distribuição de ações judiciais em que o candidato for parte.

(ii) Certidão de antecedentes criminais.

(iii) Certidões emitidas por sistemas de proteção ao crédito (SPC, SERASA etc.)

Naquela seção, a pergunta era se estas informações poderiam ser solicitadas aos candidatos como condição à sua participação em processo seletivo. Aqui, a pergunta é se o recrutador poderia pesquisar por conta própria essas mesmas informações, para uso em processo seletivo. Vale repetir que a justificativa do ponto de vista da proteção de dados depende de a legislação específica aplicável ao processo seletivo permitir a exigência de tais dados ou documentos. Assim, a orientação é:

(i) Deve ser consultado o Jurídico especializado em direito trabalhista e cível, para que se informe se a exigência é permitida do ponto de vista da legislação trabalhista ou cível aplicável ao processo seletivo, como também deve ser consultado o Encarregado de proteção de dados, para que sejam consideradas as questões de proteção de dados envolvidas.

- Currículos coletados em sites especializados

No recrutamento de colaboradores, por vezes se faz uso de sites especializados que contêm bancos de currículos. Quando um profissional cadastra seu currículo ou perfil neste tipo de site, entende-se que a finalidade almejada por este profissional é que seu currículo seja acessado e considerado para o preenchimento de vagas profissionais. Portanto, ele consente com o uso das informações ali depositadas, desde que o uso se restrinja à citada finalidade. Assim, se respeitada esta finalidade, currículos coletados em sites especializados podem ser utilizados, desde que se tome um cuidado adicional, conforme será mais bem descrito a seguir.

Na sistemática da LGPD está presente a figura da solidariedade na responsabilidade por danos decorrentes de uso ilegal de dados pessoais (Art. 42, I e II, LGPD). Nessa situação, especificamente, isso significa que, caso um site de currículos utilizado com a citada finalidade cause danos a terceiros, por descumprimento da LGPD, e a pessoa jurídica responsável pela seleção e/ou oferta de emprego concorra para a ocorrência deste dano, ela pode ser responsabilizada por sua reparação em conjunto com aquele site. A providência recomendada para evitar a incidência da responsabilidade solidária é fazer uma checagem sobre o cumprimento da LGPD por parte dos sites de oferta de currículos e vagas. Recomenda-se que o Encarregado de Dados verifique a conformidade dos sites a serem utilizados, fazendo uma lista dos sites aprovados. Ainda, recomenda-se que tal verificação de conformidade seja renovada anualmente.

6.4. O QUE FAZER COM OS DADOS NO FIM DA SELEÇÃO?

Os dados fornecidos em processo seletivo, conforme se observou anteriormente, estão subordinados a uma certa finalidade que é possibilitar a realização daquele processo. Mesmo quando o candidato a colaborador terminar por ser contratado, a finalidade subjacente ao fornecimento daqueles dados estará cumprida e não haveria mais necessidade de guardá-los. No entanto pode ser que alguns dos dados fornecidos em processo seletivo coincidam com dados a serem fornecidos em procedimento de contratação, como é o caso dos dados de identificação (RG, CPF, fotocópias destes dois documentos etc.). Caso seja conveniente em termos de rotina de trabalho, os dados deste tipo podem ser mantidos e não precisam ser solicitados novamente. Todos os dados que não serão utilizados durante a vinculação do colaborador com a pessoa jurídica responsável pela contratação e/ou vaga de emprego, tais como cartas de motivação, provas e exames realizados durante o processo de seleção, não devem ser armazenados. Se for necessária alguma espécie de checagem de informações, a partir de CVs ou cartas de motivação, por exemplo, recomenda-se que seja feita durante o processo seletivo.

ATENÇÃO!

Uma vez concluída a seleção do colaborador, a finalidade para a coleta dos dados pessoais dos candidatos terá sido suprida. Todos os dados que não forem essenciais para a fase de vinculação do colaborador devem ser eliminados.

7. LIDANDO COM DADOS DE COLABORADORES

7.1. DADOS PARA A CONTRATAÇÃO

(i) Coleta

Diferentes tipos de vinculação, estabelecidos entre a pessoa jurídica contratante ou ofertante da vaga e seus colaboradores, podem possuir especificidades quanto aos dados pessoais envolvidos. Nesse sentido, verifica-se que os dados exigidos para a vinculação no caso de um colaborador regido pelo sistema de CLT não irão coincidir, em sua integralidade, com os dados exigidos para o cadastro dos estagiários ou de aprendizes. Essa seção, portanto, tem como objetivo apresentar exemplificativamente os dados que devem ser coletados. Caberá, dessa

forma, a Unidade de RH responsável pela vinculação avaliar se é indispensável a coleta de mais algum dado específico a depender da vinculação pretendida.

DICA:

A finalidade da coleta, neste caso, é a constituição do vínculo entre a Contratante e o colaborador. Deste modo, devem ser coletados somente os dados que sejam necessários à constituição deste vínculo, a depender de qual seja ele no caso concreto.

A partir do momento em que o colaborador é aprovado no processo seletivo podem ser coletados, para fins de exemplificação, os seguintes dados pessoais:

- ✓ Nome
- ✓ RG
- ✓ CPF
- ✓ Dados bancários para fins de pagamento
- ✓ Endereço
- ✓ Número de PIS/PASEP/NIS
- ✓ Carteira de trabalho
- ✓ Foto

A coleta dos dados supracitados encontra respaldo, em um primeiro momento, na base legal da execução de contrato. Segundo esta base, podem ser tratados dados pessoais quando a finalidade for a de permitir a execução de um contrato no qual o titular de dados possui interesse na execução (artigo 7, V da LGPD). Além dos dados citados acima, há uma série de outros documentos que podem ser solicitados, conforme a posição do colaborador, nos quais constam diversos dados pessoais. Novamente ressalta-se que nenhum dado pessoal pode ser exigido caso este não esteja atrelado à função a ser exercida pelo colaborador, sendo ele estritamente necessário para a elaboração do contrato/vínculo formal a ser estabelecido entre a pessoa jurídica ofertante do emprego e/ou responsável pela vaga e o colaborador.

ATENÇÃO! Recomenda-se, portanto, que sejam solicitados os dados estritamente necessários para a realização do contrato.

Vale aqui mencionar a exigência, para fins de contratação regidas pela CLT, a realização de um exame médico admissional. Mesmo sendo produzido um dado de saúde e, portanto, um dado sensível, este não necessita de qualquer consentimento adicional, tendo em vista o amparo legal para sua coleta. Cabe também aqui mencionar os dados utilizados para a inclusão no sistema E-Social[2] . Sendo um sistema informatizado da administração pública, cujo abastecimento com informações trabalhistas, fiscais e previdenciárias é obrigatório, o registro de dados pessoais de empregados feito pela pessoa jurídica responsável pelo processo seletivo em tal sistema está coberto pela base legal do cumprimento de obrigação regulatória (Art. 7, II, LGPD). Nos casos em que a CLT ou outra fonte regulatória de direito solicitar que, para a realização de um vínculo de um colaborador seja fornecido algum dado sensível, tal requisição estará respaldada pela

[2] Sistema informatizado da Administração Pública que regula e registra vínculos trabalhistas. Todas as informações nele contidas estão protegidas por sigilo. Mais informações em <https://login.esocial.gov.br/login.aspx>.

base da obrigação legal (artigo 7, II da LGPD) e, portanto, poderá ser fornecida sem qualquer requisito adicional.

(ii) Armazenamento

O tempo de armazenamento dos dados tratados deve ser equivalente ao tempo de vigência do vínculo estabelecido entre o colaborador e a responsável pela contratação ou vaga, somado ao prazo de guarda após o término da relação. Passado esse prazo, a finalidade do armazenamento estará exaurida, salvo nas hipóteses em que existir uma previsão legal que regule o armazenamento por prazo superior (Art. 7, II, da LGPD). Cabe ressaltar que dados diferentes podem ter prazos de guarda diferentes, com fundamento em legislações diferentes. Por exemplo, o prazo de guarda de documentos em razão de possíveis reclamações trabalhistas será diferente do prazo de guarda de informações financeiras por razões tributárias

ATENÇÃO!

- Caso haja litígio judicial, os dados pessoais do colaborador que seja parte do processo devem ser guardados pelo menos até que haja o trânsito em julgado do referido litígio, cabendo consultar o setor jurídico e o Encarregado sobre a conveniência de guarda por prazo superior em virtude, por exemplo, da possibilidade de ação rescisória;

- Caso haja previsão legal ou regulatória específica sobre prazos de armazenamento de dados, estas devem ser cumpridas

(iii) Compartilhamento

O compartilhamento dos dados é necessário para a execução do contrato de vinculação estabelecido entre o colaborador e a pessoa jurídica contratante ou ofertante da vaga. Nesse sentido, tem-se que muitas vezes, o compartilhamento, ao menos interno à pessoa jurídica contratante ou ofertante da vaga, é necessário para que o próprio colaborador possa realizar os trabalhos para os quais foi contratado. Por exemplo, pode ser indispensável que o colaborador tenha seus dados compartilhados com a portaria, para que este tenha acesso as instalações da pessoa jurídica contratante ou ofertante da vaga. Ainda, pode ser necessário que exista o compartilhamento com a unidade competente dentro da pessoa jurídica contratante ou ofertante da vaga, para que seja feito um crachá para o colaborador. O compartilhamento também pode ser feito externamente à pessoa jurídica contratante ou ofertante da vaga, por exemplo, quando necessário para o cumprimento de obrigação legal (Art. 7, II, da LGPD) ou regulatória pela mesma Instituição. Nesse caso, não é necessária a obtenção de consentimento. Nesta categoria se enquadram, por exemplo, as obrigações de enviar dados ao Ministério da Economia/Secretaria do Trabalho ou ao Ministério da Saúde, estabelecidas em legislação específica.

Nesse sentido, destaca-se que, os compartilhamentos internos de dados pessoais, por mais simples que sejam, devem seguir alguns requisitos mínimos estabelecidos pela LGPD para que sejam realizados de maneira considerada lícita. Dois desses requisitos estão dispostos nos Art. 6º, 7º e 11 da Lei: (i) a observância aos princípios de proteção de dados pessoais, e (ii) a existência de uma base legal para a realização do tratamento. Frisa-se, deste modo, os princípios da finalidade, adequação, necessidade, transparência e segurança. Dessa forma todos os

compartilhamentos de dados pessoais realizados internamente pela Unidade de RH com outras unidades da pessoa jurídica contratante ou ofertante da vaga devem obedecer, principalmente:

(i) Princípio da finalidade: o propósito do tratamento deve ser informado ao titular de dados pessoais. Importante notar que esses propósitos também devem ser legítimos, específicos e explícitos, e que quaisquer tratamentos a serem realizados com os dados posteriormente não podem ser realizados de forma incompatível com as finalidades anteriormente estabelecidas;

(ii) Princípio da adequação: o tratamento a ser realizado deve ser compatível com as finalidades informadas ao titular;

(iii) Princípio da necessidade: apenas os dados pertinentes, proporcionais e não excessivos em relação às finalidades podem ser utilizados para o tratamento;

(iv) Princípio da transparência: ao titular devem ser concedidas informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os agentes de tratamento;

(v) Princípio da segurança: devem ser utilizadas as medidas técnicas e administrativas adequadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Alguns outros artigos, ao longo da LGPD, reforçam a necessidade de atendimento ao cumprimento desses princípios, inclusive no caso específico do compartilhamento de dados. É o caso do art. 9º, V, que estabelece o direito de o titular de dados ter acesso a informações relativas ao uso compartilhado de dados que é realizado pela Controladora e a finalidade desse tratamento. Ou seja, no momento da coleta dos dados pessoais junto aos titulares, é necessário informá-lo, de maneira clara, precisa, em linguagem acessível e de fácil compreensão, sobre quais dados pessoais serão tratados, para quais finalidades, e quais tratamentos serão feitos – incluindo os compartilhamentos que serão realizados entre as unidades internas da pessoa jurídica contratante ou ofertante da vaga. É importante que essa definição não seja feita de maneira genérica, i.e., deve haver uma listagem de todos os locais da Instituição para os quais os dados poderão ser encaminhados. Ainda, deve-se garantir que apenas os dados pessoais estritamente necessários para a consecução da finalidade do tratamento sejam compartilhados, evitando que dados excessivos e desnecessários sejam encaminhados às outras unidades da pessoa jurídica contratante ou ofertante da vaga.

Por fim, cabe dizer que a LGPD também traz, em seu art. 46, e em alinhamento com o princípio da segurança, disposição sobre a necessidade de que os agentes de tratamento adotem medidas de segurança (técnicas e administrativas) que sejam capazes de 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. Quando a pessoa jurídica contratante ou ofertante da vaga, no papel de Controladora de dados pessoais, contratar com terceiros a realização de atividades que envolvam tratamento de dados pessoais (por exemplo, contrato de armazenamento de documentos, digitais ou físicos), deve exigir do terceiro contratado os cuidados de segurança cabíveis. As medidas de segurança citadas anteriormente também devem ser aplicadas ao contexto do compartilhamento de dados pessoais entre órgãos internos da pessoa jurídica contratante ou ofertante da vaga. Dessa forma, os dados pessoais devem ser compartilhados apenas com pessoas, áreas, unidades, subunidades e órgãos devidamente autorizados a receber tais dados e que tenham ingerência e/ou contato direto com os tratamentos a serem realizados com eles. Ademais, é necessário que os dados sejam compartilhados de uma maneira segura, por vias seguras, evitando, por exemplo, que eles sejam

compartilhados por meio de arquivos como planilhas ou por e-mail. Em sendo possível, os dados pessoais devem ser mantidos nos ambientes de servidores próprios, e compartilhados pelos meios aprovados e considerados como adequados, em termos de segurança, pela área de tecnologia da informação. Uma boa prática recomendada é que a área de tecnologia da informação da pessoa jurídica contratante ou ofertante da vaga estabeleça as diretrizes técnicas, padrões e medidas de segurança a serem adotadas, de forma que possam ser aplicadas pelas colaboradoras nos casos e rotinas de trabalho concretas.

7.2. DADOS GERADOS NO ACOMPANHAMENTO DA ATIVIDADE PROFISSIONAL DOS COLABORADORES

(i) Coleta

São diversos os dados pessoais que podem ser gerados durante a constância do vínculo entre a pessoa jurídica contratante ou ofertante da vaga e seus colaboradores. Por exemplo, registros de entrada e saída de prédios, avaliações de desempenho, registros de pagamentos etc. Estes dados, em regra, são gerados como forma de instrumentalizar e fiscalizar o cumprimento/execução do contrato em que se baseia a relação entre pessoa jurídica contratante ou ofertante da vaga e colaborador (artigo 7, V da LGPD). Portanto, não se faz necessário o consentimento da coleta destes dados para que estes sejam tratados. Ressalta-se que, ao se coletar dados nesta hipótese, persiste a necessidade de se observar a finalidade da coleta dos dados, bem como a adequação/necessidade dos dados pretendidos para o cumprimento de tal finalidade.

(ii) Armazenamento

Existem muitos dados que são gerados na duração do contrato de trabalho que não necessitam ser armazenados após o seu término. Por exemplo, o dado referente ao local que determinado profissional se posiciona nas salas de trabalho ou locais de trabalho da pessoa jurídica contratante ou ofertante da vaga (mapa de lugares). Os dados pessoais, portanto, só devem ser mantidos após o fim do vínculo entre colaborador e pessoa jurídica contratante ou ofertante da vaga: (i) caso digam respeito a um tema que pode ser invocado pela via administrativa ou judicial, devendo ser armazenados pelo prazo prescricional das ações que podem ser ajuizadas; (ii) caso haja litígio judicial em andamento ou no encerramento do vínculo, os dados devem ser guardados enquanto persistir o litígio; (iii) caso haja previsão legal ou regulatória específica sobre prazos de armazenamento de dados, estas devem ser cumpridas (iv) na hipótese de haver interesse da instituição. Destaca-se aqui que determinados dados pessoais que passam a existir durante a constância do vínculo profissional são dados sensíveis ou equiparados a dados sensíveis, gerados durante o desenvolvimento da atividade profissional (tais como dados de pagamento, por exemplo). Caso haja vazamento desses dados, podem ocasionar graves danos ao titular de dados, motivo pelo qual devem ser tratados com especial cuidado[3]. Para o

[3] Ressalte-se aqui o entendimento, adotado pela equipe que elaborou este e os demais Guias relacionados, de que dados financeiros devem ter tratamento análogo ao de dados sensíveis nas hipóteses em que eles puderem ser usados para discriminar o titular de dados. Neste sentido, serão equiparados a dados sensíveis.

armazenamento dos referidos dados sempre é necessário observar as recomendações de segurança adicionais citadas na seção 6, notadamente que: (i) um número restrito de pessoas tenha acesso às informações obtidas; (ii) esses dados fiquem em um servidor que assegure segurança e proteção às informações; e (iii) esses dados sejam armazenados, preferencialmente, criptografados. Recomendações de segurança análogas valem para os dados registrados em papel. Ainda, vale observar que as medidas de segurança e as especificações técnicas para sua implementação, conforme boa prática recomendada anteriormente, poderão ser definidas e padronizadas pela área de tecnologia da informação da pessoa jurídica contratante ou ofertante da vaga. Em suma, tem-se que é possível o armazenamento de dados por tempo determinado de ex-colaboradores. Esse armazenamento pode ou não estar condicionado ao prazo previsto na obrigação legal que fundamenta tal armazenamento. Uma vez terminado o contrato e findada a necessidade de armazenamento para fins legais, não cabendo qualquer outra exceção de tratamento que justifique esse armazenamento, tem-se que a finalidade deste estará exaurida e tais dados devem ser eliminados.

(iii) Compartilhamento

O compartilhamento também está limitado pela finalidade para a qual os dados foram coletados (instrumentalizar e fiscalizar o cumprimento do contrato em que se baseia a relação entre pessoa jurídica contratante ou ofertante da vaga e colaborador), e por sua necessidade ao cumprimento desta finalidade. Os compartilhamentos internos que sejam necessários ao cumprimento de tais finalidades está, portanto, coberto pela base legal do Art. 7, V, LGPD). Seria o caso, por exemplo, do compartilhamento de informações sobre colaboradores com diretores ou gestores, para que estes avaliem desempenho ou tomem decisões gerenciais. Por outro lado, o compartilhamento externo está autorizado quando for necessário para o cumprimento de obrigação legal ou regulatória pela pessoa jurídica contratante ou ofertante da vaga. Nessa categoria se enquadram, por exemplo, algumas obrigações de enviar dados ao Ministério da Economia/Secretaria do Trabalho, Ministério da Justiça ou Ministério Público, estabelecidas em legislação específica. Mais uma vez, aplicam-se todas as considerações feitas quanto ao tratamento de compartilhamento previstas na seção 7.1. Cabe aqui considerar ainda a hipótese de um recrutador requerer que sejam compartilhadas informações referentes a um funcionário da pessoa jurídica contratante ou ofertante da vaga para um processo de admissão, situação em que ele estaria pleiteando o compartilhamento externo de dados de colaboradores de tal pessoa jurídica contratante ou ofertante da vaga. Nesse sentido, todas as recomendações quanto a compartilhamento externo deveriam ser seguidas antes de se disponibilizar dados como uma carta de recomendação ou o histórico de um funcionário na pessoa jurídica contratante ou ofertante da vaga em questão.

7.3. DADOS GERADOS EM SINDICÂNCIAS OU PROCESSOS ADMINISTRATIVOS INTERNOS

Os dados gerados em sindicâncias ou processos administrativos internos podem ser tratados independentemente do consentimento do titular. Isso porque são dados gerados para assegurar o exercício regular de processos jurídicos ou administrativos (artigo 7, VI da LGPD). Mesmo sem a necessidade de obtenção de consentimento, permanecem, entre outras, as limitações de finalidade e necessidade. A finalidade, neste caso, seria a de esclarecer a responsabilidade sobre os fatos que deram origem à sindicância ou processo administrativo internos.

7.4. DADOS RELACIONADOS À CONCESSÃO DE BENEFÍCIOS

Uma pessoa jurídica contratante ou ofertante da vaga pode conceder benefícios específicos a certas categorias de colaboradores, como planos de saúde, auxílio creche ou plano de previdência privada. Quanto à concessão de benefícios deste tipo, no que diz respeito à proteção de dados pessoais, é importante dar atenção a duas situações distintas. Em uma primeira hipótese, tem de se considerar o caso de o benefício oferecido estar relacionada à parceria estabelecida entre a pessoa jurídica contratante ou ofertante da vaga e uma terceira empresa, que efetivamente concede o benefício (geralmente é o caso de planos de saúde, por exemplo).

Nesses casos, a pessoa jurídica contratante ou ofertante da vaga geralmente tem, tão somente, de inscrever os seus colaboradores para que estes recebam o benefício garantido pela terceira parte. Ressalta-se que, nestes casos, a transferência de dados está limitada à finalidade, que é a inscrição do colaborador junto ao administrador do benefício (seguradora, plano de saúde etc.). Portanto, os dados a serem transferidos são apenas aqueles estritamente necessários ao cumprimento desta finalidade. Ainda, tem-se que é necessário o consentimento dos colaboradores, que têm de anuir, quando forem preencher formulário de inscrição, com os tratamentos de dados que a administração do benefício demanda. Além disso, a pessoa jurídica contratante ou ofertante da vaga, na hipótese supracitada, não deve receber da empresa administradora do benefício nenhum dado que não seja essencial à fiscalização da prestação do serviço, especialmente quando se tratar de dados sensíveis. A segunda hipótese prevê as situações em que a própria pessoa jurídica contratante ou ofertante da vaga conceda ou administre algum benefício aos seus colaboradores sem, com isso, contratar uma terceira para prestar esse serviço. Nessas hipóteses, verifica-se que a própria pessoa jurídica contratante ou ofertante da vaga provavelmente já possuirá os dados necessários para o cadastramento no serviço, mas, ainda assim, depende que seja dado o consentimento por parte do colaborador titular de dados para que seus dados sejam cadastrados no benefício concedido. Isso porque, não é possível presumir que, ao entregar seus dados para a contratação, o colaborador estivesse de acordo e tivesse consentido com o tratamento desses dados com a finalidade de concessão de algum benefício em especial. Em ambos os casos, na hipótese de o benefício se estender também aos familiares dos colaboradores, tem-se que estes deveriam indicar seu consentimento com o tratamento de tais dados. O cônjuge de colaborador, por exemplo, que for ser inscrito em plano de saúde como beneficiário, deve manifestar seu consentimento com os tratamentos de dados que sejam necessários à administração do benefício. Ainda, na hipótese do benefício se estender aos filhos adolescentes, recomendasse que os pais sejam os responsáveis por indicar o consentimento dos menores de 16 anos, consoante previsto no Guia de Proteção de Dados Pessoais: Crianças e Adolescentes. No mais, mantem-se todas as recomendações quanto a compartilhamentos internos já incorporados a este Guia.

8. LIDANDO COM DADOS DE EX-COLABORADORES

Como já pontuado anteriormente, todos os dados pessoais tratados durante o vínculo estabelecido com os colaboradores possuem um “ciclo de vida”. Isso significa que esses dados não podem ser mantidos indeterminadamente nos bancos de dados da pessoa jurídica contratante ou ofertante da vaga. Nesse sentido, após o término do vínculo estabelecido entre

o colaborador e a pessoa jurídica contratante ou ofertante da vaga, os dados devem ser excluídos da base de dados. É também o que prevê o Art. 16 da LGPD.

Consoante disposto acima, tem de ser considerada também a hipótese de um ex-colaborador ingressar com uma ação trabalhista contra a pessoa jurídica contratante ou ofertante da vaga, situação em que a mesma pessoa jurídica contratante ou ofertante da vaga necessitaria de acesso a dados do ex-colaborador, gerados na constância do vínculo, para poder elaborar sua defesa. Justamente por esse motivo, o próprio Art. 16 estabelece exceções quanto à eliminação dos dados após o tratamento ter sido encerrado e, no caso, após o vínculo com o colaborador ter se encerrado. Em razão do exposto, importante esclarecer exatamente quais dados de ex-colaboradores, armazenados pela Unidade de RH, devem ser excluídos, quais devem ser mantidos e por quanto tempo esses dados devem continuar armazenados após o término do vínculo gerado com a instituição. Segundo o Art. 16, inciso I, da LGPD, o armazenamento após o tratamento é permitido nas hipóteses em que exista previsão legal ou que exista a necessidade do armazenamento para funções regulatórias da Controladora. Nesse sentido importante destacar que a legislação estabelece que o prazo para o ingresso de ações trabalhistas prescreve em dois anos após o término da relação estabelecida (Constituição Federal, Artigo 7 XXIX). De mesmo modo importante considerar que em ações de cunho trabalhista são analisadas uma série de dados pessoais de ex-funcionários, tais como dados de saúde, dados de frequência, dados de dias abonados, de férias gozadas etc. Por esse motivo, com fundamento na base legal da legislação trabalhista, recomenda-se que os dados sejam eliminados apenas após o prazo para o ingresso de alguma ação trabalhista face à pessoa jurídica contratante ou ofertante da vaga. No que atine a dados do sistema financeiro e dados da contabilidade, tem-se que estes devem ser armazenados até que o prazo para uma ação de cunho civil ou tributária possa ser ajuizada face à administração da pessoa jurídica contratante ou ofertante da vaga.

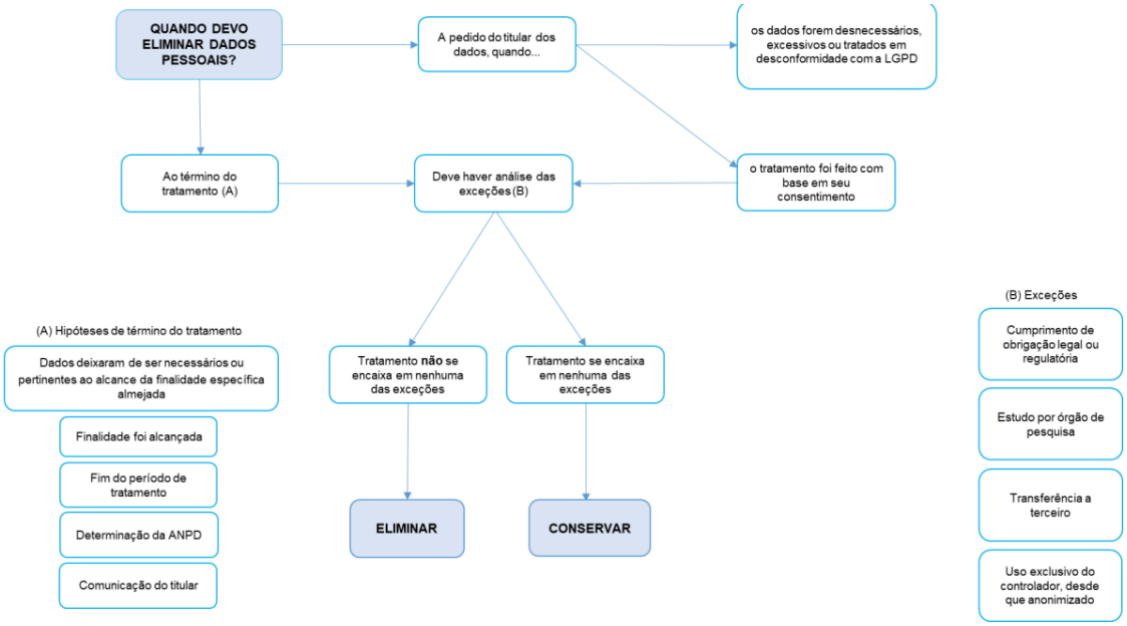
- Dados relativos ao registro da história da pessoa jurídica contratante ou ofertante da vaga

Uma pessoa jurídica contratante ou ofertante da vaga às vezes possui o interesse em registrar sua própria história. Uma parte importante desta história se constitui na trajetória de pessoas que contribuíram especialmente para as realizações da pessoa jurídica, como fundadores ou administradores. Os dados necessários para preservar à memória da instituição podem ser mantidos numa base de dados, desde que com o consentimento do titular. O consentimento pode ser colhido no momento da contratação. Ainda, em casos pontuais, em que a história do colaborador esteja demasiadamente vinculada à história da instituição, pode-se dizer que o armazenamento de dados deste tipo corresponde a realização de pesquisa histórica e, por isso, estaria autorizado pela base legal do Art. 7, IV, LGPD.

Por fim, considera-se a hipótese de a pessoa jurídica contratante ou ofertante da vaga ter a pretensão apenas de ter uma estimativa relativa à capacitação de seus colaboradores. Por exemplo, a pessoa jurídica pode ter como objetivo apenas saber quantas pessoas com formação em nível superior passaram por sua pessoa jurídica como colaboradores. Nesses casos tem-se a alternativa de realizar o registro de sua história pode se dar através do armazenamento de dados agregados ou anonimizados.

9. ELIMINAÇÃO DE DADOS

Em todos os tópicos supra listados existe a previsão eliminação de certos dados pessoais, quando possível e quando inexistir uma base legal que impeça a referida eliminação. Importante, nesse sentido, retomar as hipóteses cabíveis de eliminação. A LGPD traz, em seu art. 5º, XIV; art. 15º; art. 16º; e art. 18º, incisos IV e VI, disposições sobre a eliminação de dados pessoais. Dessas disposições, vamos dar enfoque em três: (i) quando ela for solicitada pelo titular de dados pessoais, quando o tratamento foi feito com base em seu consentimento; (ii) quando os dados utilizados forem desnecessários, excessivos ou tratados em desconformidade com a LGPD; ou (iii) quando houver o término do tratamento dos dados. No atinente a eliminação em função do pedido do titular (i), tem-se que esta será aplicável aos casos de processo seletivo. Como ficou determinado, nesses casos a base legal é o consentimento, de modo que, se o titular pedir a eliminação dos dados, ela deverá ser realizada. Destaca-se aqui que a hipótese em caso de eliminação em decorrência do pedido do titular não é aplicável aos dados tratados na constância do vínculo contratual entre o Colaborador ao RH, visto que a base legal aplicável, nestes casos, é a de execução de contrato, sendo a manutenção essencial para o desenvolvimento da função das unidades. Quando se tratar de (ii) solicitação de dados desnecessário, excessivo ou em desconformidade com a LGPD, por sua vez, estes dados devem ser encaminhados ao Encarregado, que deverá recomendar as medidas necessárias. Existe, por fim, a eliminação decorrente do término do tratamento (iii). Nesses casos, quando inexistir a necessidade de guarda dos documentos, consoante dispostos nas regras dispostas nos tópicos acima, estes devem ser eliminados. Destaca-se que em qualquer uma das possibilidades de eliminação (i) e (ii), o agente de tratamento deve realizar uma avaliação de exceções em que os dados pessoais podem ser conservados, a despeito do pedido do titular de dados ou do término do tratamento. As exceções dizem respeito às seguintes finalidades: (a) o cumprimento de obrigação legal ou regulatória; (b) os dados serão utilizados por órgão de pesquisa; (c) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei; (d) uso exclusivo da Controladora, vedado seu acesso por terceiro. O fluxograma abaixo pode auxiliar a compreender as situações de eliminação de dados pessoais:



A LGPD também traz a possibilidade, nos casos em que a base legal utilizada é a do consentimento, de o titular de dados exercer o direito de revogá-lo, a qualquer tempo, sendo necessário corrigir todos os tratamentos realizados sob a autorização do consentimento. Além disso, o titular também poderá solicitar a eliminação desses dados. Nesse caso, a Unidade de RH

da pessoa jurídica contratante ou ofertante da vaga deverá fazer uma análise da situação em concreto, considerando o pedido de eliminação dos dados pessoais de forma a analisar se (i) a rotina permite que os dados sejam eliminados; e (ii) as possíveis consequências da eliminação para o próprio titular de dados. Sobe as formas de eliminação, destaca-se que estas terão de seguir as políticas próprias de descarte de dados armazenados em papel e em mídia digital.

10. CONSIDERAÇÕES FINAIS

A atividade de gestão de Recursos Humanos, conforme se pode ver, envolve uma série de tratamentos de dados pessoais, inclusive dados pessoais sensíveis. Ao cuidarmos neste Guia das principais rotinas que envolvem tratamentos de dados pessoais, exemplificativamente, pretendeu-se orientar especificamente sobre situações mais corriqueiras. Ao mesmo tempo, através da constante repetição de conceitos na análise destas situações e nas recomendações feitas a partir dela, pretendeu-se ajudar na preparação daqueles que lidam com gestão de recursos humanos para lidarem com situações diferentes das que aqui foram abordadas. Assim, em retrospecto, é fundamental que se retenham alguns pontos que foram enfatizados ao longo do Guia. Primeiro, que existem diversas bases que se mostram adequadas no tratamento de dados na Unidade de RH, dentre elas o legitimo interesse, a execução de contrato, o cumprimento de obrigação legal e o consentimento, que sempre deve ser buscado quando não houver outra base legal que permita o tratamento do dado. A obtenção do consentimento, por sua vez, depende da prestação de informações sobre todas as operações de tratamento que se pretende realizar, junto da declaração das finalidades atreladas às operações de tratamento informadas. Depende também da manifestação clara de vontade do titular de dados. Uma vez que o ônus de provar que o consentimento foi obtido nas condições dispostas na LGPD, é desejável, quando couber, que se registre o consentimento de forma que possa servir como tal prova. As operações de tratamento ficam limitadas pelas finalidades informadas, e por sua necessidade para o cumprimento de tais finalidades. Assim, sempre deve haver um controle de finalidade/necessidade na realização de quaisquer operações de tratamento. Apesar da segurança representada pelo consentimento como base legal, há tipos de dados e operações de tratamento às quais se aplicam outras bases legais de modo bastante claro, como o cumprimento de obrigação legal ou regulatória em diversas rotinas comuns à gestão de recursos humanos. Com efeito, há diversas obrigações determinadas pela legislação trabalhista ou pela regulação do sistema federal de ensino, por exemplo, que equivalem a certas operações de tratamento de dados pessoais. Nestes casos, a pessoa jurídica contratante ou ofertante da vaga está dispensada da obtenção do consentimento para realizar tais tratamentos. Os dados sensíveis, mesmo quando obtidos sob uma base legal incontroversa, demandam cuidados adicionais tanto no juízo de finalidade/necessidade dos tratamentos a serem realizados quanto nas medidas de segurança da informação a serem adotadas. Por fim é importante ter em mente que os dados pessoais possuem aquilo que se chama de ciclo de vida em relação a uma certa Controladora. Isto é, a Controladora coleta os dados, os trata e os armazena pelo tempo suficiente para realizar as finalidades atreladas à base legal que serviu à sua coleta. Quando essas finalidades são atingidas, encerram-se os tratamentos, e quando se dá este encerramento, os dados devem, a menos da ocorrência de condições específicas, serem eliminados. Esta eliminação, por sua vez, deve se dar com observância dos padrões de segurança de informação aplicáveis.

11 – MODELOS UTILIZADOS EM RECURSOS HUMANOS

Os modelos abaixo são utilizados nos processos seletivos do CONTROLADOR.

Alguns vínculos entre colaboradores e a parte contratante, seja diretamente ou por terceirização, para serem efetivados, estão condicionados a um processo de seleção. A realização desse processo de seleção envolve uma série de tratamentos de dados pessoais do candidato interessado. Justamente por esse motivo, a seleção é feita em observância à LGPD. Cumpre esclarecer que as recomendações aqui dispostas são aplicáveis tanto caso o colaborador seja admitido, bem como na hipótese de o candidato não ser admitido.

Na seleção de colaboradores, todos os dados pessoais coletados estão diretamente relacionados ao processo seletivo, sendo estritamente necessários para que ele seja realizado. Nestes casos, existe uma clara finalidade em obter dados pessoais que revelem meios de identificar o candidato, bem como seu enquadramento à vaga pretendida. Razoável, portanto, coletar dados como: RG, CPF, e-mail, telefone de contato, pedido para que seja indicada a formação do candidato, experiência prévia na área etc. Em alguns casos bastante específicos, quando previamente informado ao participante, os dados obtidos por meio de certidões merecem consideração especial, por existirem limitações à sua exigência em processos seletivos, especialmente decorrentes do Direito do Trabalho. Tais dados são integralmente respeitados no presente processo seletivo, e somente são recolhidos dentro dos limites dos entendimentos da jurisprudência dos tribunais brasileiros e da legislação brasileira, sendo previamente informados ao candidato, quando aplicável à vaga, na primeira página do Termo de Consentimento para Tratamento de Dados Pessoais em Processos Seletivos, com as finalidades indicadas, e dentro dos limites da legislação e jurisprudência brasileira, principalmente no ponto de vista trabalhista, para alguns cargos específicos.

TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS EM PROCESSO SELETIVO DE CONTRATAÇÃO

DESCRIÇÃO DA VAGA DE EMPREGO: [DESCRIÇÃO COMPLETA]

QUALIFICAÇÃO DO OFERTANTE DA VAGA: [QUALIFICAÇÃO COMPLETA]

QUALIFICAÇÃO DA PESSOA JURÍDICA ONDE SERÁ EXERCIDO O TRABALHO:

FERRANTE ADVOGADOS

DADOS PESSOAIS DO CANDIDATO – FORNECIDOS PELO CANDIDATO:

1. Nome completo do candidato: _____ (FINALIDADE: IDENTIFICAÇÃO DO CANDIDATO)
2. CPF: _____ (FINALIDADE: IDENTIFICAÇÃO DO CANDIDATO E EVITAR HOMONÍMIAS)
3. Telefone para contato: _____ (FINALIDADE: CONTATO COM CANDIDATO)
4. E-mail para contato: _____ (FINALIDADE: CONTATO COM CANDIDATO)
5. [demais dados solicitados, dentro dos parâmetros de necessidade e adequação]: (FINALIDADE: ESPECIFICAR)

EU, candidato acima qualificado, para a vaga de emprego descrita acima, conforme especificações acima:

1. Declaro que **CONCORDO COM O TRATAMENTO DE MEUS DADOS PESSOAIS PARA FINALIDADE EXCLUSIVA DE REALIZAR AÇÕES RELACIONADAS AO RECEBIMENTO DE CURRÍCULO, AVALIAÇÃO, SELEÇÃO, MANUTENÇÃO DE CURRÍCULO E DADOS PESSOAIS EM BANCO DE DADOS PARA FUTURAS OPORTUNIDADES DE SELEÇÃO E EVENTUAL RECRUTAMENTO PARA PARTICIPAÇÃO EM PROCESSOS DE ADMISSÃO** para compor o quadro de colaboradores ofertado pela empresa acima qualificada, para trabalho na pessoa jurídica acima especificada, conforme o quanto disposto no presente termo e seu(s) anexo(s).
2. **DECLARO QUE, ANTES DE MINHA CONCORDÂNCIA, CONFORME ESPECIFICADO ACIMA, LI, TOMEI CIÊNCIA E COMPREENDI A INTEGRALIDADE DO QUANTO ESPECIFICADO NO PRESENTE TERMO DE CONSENTIMENTO E SEU(S) ANEXO(S), de modo que assino o presente termo de maneira totalmente livre e esclarecida.**
3. **DECLARO QUE ESTOU CIENTE DAS CONSEQUÊNCIAS DE NÃO CONSENTIR PARCIALMENTE OU TOTALMENTE COM O FORNECIMENTO OU COLETA DE DADOS CONFORME ESPECIFICADO NO PRESENTE TERMO E SEUS ANEXOS**, sendo as consequências de não aceite de tratamento de dados pessoais as seguintes:

- **Caso não concorde de maneira integral: o candidato não será considerado para a vaga pretendida e será desconsiderado no processo seletivo.**
- **Caso não concorde de maneira parcial, com dados pessoais que não são considerados essenciais para a identificação do candidato e para o contato com o candidato, tais dados não informados não serão, como consequência lógica, considerados no processo avaliativo.**

O tratamento dos dados pessoais poderá ser realizado para possibilitar o processo seletivo da vaga, possível estabelecimento de vínculo contratual e todos os atos que decorram da eventual relação de trabalho a ser firmada entre o CANDIDATO e o CONTROLADOR.

DO COMPARTILHAMENTO E SEGURANÇA DOS DADOS

CONTROLADOR fica desde já autorizado a compartilhar os dados pessoais do CANDIDATO com sua área interna de gestão de pessoas, ou empresa terceirizada, inclusive com o gestor da área que deu origem à vaga, com empresas de recrutamento e seleção, com redes sociais de negócios e com empresas terceiras que fornecem licença de software para armazenamento e gestão de dados.

CONTROLADOR responsabiliza-se pela supervisão, no caso de terceiros gerenciadores da vaga, ou manutenção 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.

Em conformidade ao artigo 48 da Lei nº 13.709, o CONTROLADOR comunicará ao CANDIDATO e à Autoridade Nacional de Proteção de Dados – ANPD a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao CANDIDATO.

DO TÉRMINO DO TRATAMENTO DOS DADOS

O CONTROLADOR poderá manter e tratar os dados pessoais do CANDIDATO durante todo o período em que estes forem pertinentes ao alcance das finalidades listadas neste termo ou em razão de obrigação legal.

O CANDIDATO poderá solicitar ao CONTROLADOR, a qualquer momento, que sejam eliminados seus dados pessoais por meio do e-mail do Data Protection Officer do CONTROLADOR: fbrunetti@terra.com.br, sendo que sua solicitação será considerada de acordo com as leis aplicáveis.

DOS DIREITOS DO CANDIDATO

O CANDIDATO tem direito a obter do CONTROLADOR, em relação aos dados por ele tratados, a qualquer momento e mediante requisição:

- confirmação da existência de tratamento;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei nº 13.709;
- portabilidade dos dados, mediante requisição expressa;
- eliminação dos dados pessoais tratados com o consentimento do CANDIDATO, exceto nas hipóteses previstas no artigo 16 da Lei nº 13.709;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- revogação do consentimento, nos termos do § 5º do artigo 8º da Lei nº 13.709.

DIREITO DE REVOGAÇÃO DO CONSENTIMENTO

Conforme disposto acima, este consentimento poderá ser revogado pelo CANDIDATO, a qualquer momento, mediante solicitação ao CONTROLADOR, ou empresa representante do processo seletivo relacionada ao CONTROLADOR.

Ciente e de acordo do candidato.

ANEXO IV – CONTRATO DE TRATAMENTO DE DADOS PESSOAIS (“CTD”)

O presente contrato abaixo será utilizado em relação a todo e qualquer parceiro e/ou contratado da FERRANTE ADVOGADOS como meio de mitigação e prevenção de riscos em relação à LGPD.

O presente Contrato de Tratamento de Dados (“CTD”) faz parte do Contrato entre

FERRANTE ADVOGADOS

(doravante denominada “Controladora de Dados”)

E

QUALIFICAÇÃO COMPLETA DA EMPRESA OU PARCEIRO DE SERVIÇOS (doravante denominada “Operadora de Dados Pessoais”).

O presente CTD reflete o acordo das Partes em relação ao tratamento de dados pessoais pela Operadora de Dados Pessoais durante a prestação dos Serviços ou relação comercial entre as partes, conforme contrato anteriormente assinado, e em conformidade com a legislação de proteção de dados aplicável.

1. **Obrigações e Direitos da Operadora de Dados Pessoais**

1.1. As partes acordam que por conta principalmente, mas não somente, do art. 45 da LGPD (Lei Geral de Proteção de Dados - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.), caso alguma das partes seja processada judicialmente ou administrativamente por conta de alguma violação relacionada à LGPD que decorreu de culpa, ato ou fato da outra parte ou de responsabilidade da parte Controladora, nos termos do quanto definido pela LGPD e/ou ANPD, poderá a parte que foi demandada judicialmente ou administrativamente sem culpa requerer ação regressiva de ressarcimento contra a outra parte que deu causa à ação judicial ou processo administrativo, incluindo todos os gastos em que incorreu a parte demandada, inclusive com advogados e os valores relacionados à condenação, honorários sucumbenciais e custos com processo, ou custear, a requerimento da parte demandada sem culpa, todos os gastos advocatícios ou decorrentes do processo judicial e/ou administrativo em questão.

1.2. A Operadora de Dados Pessoais, por meio deste, tratará eventuais dados pessoais decorrente das relações contratuais entre as partes, de acordo com os termos do presente CTD, para o único objetivo de cumprir o Contrato, e nos termos das políticas da Controladora de Dados, aos quais declara ter tido acesso.

1.3. A Operadora de Dados Pessoais deverá processar somente os dados pessoais mediante obedecimento integral da LGPD e o quanto consta do presente Contrato, incluindo seus anexos.

1.4. A Operadora de Dados Pessoais deverá garantir que as pessoas autorizadas a tratar os dados pessoais se comprometeram com a confidencialidade ou estão sob uma obrigação legal de confidencialidade e que foram apropriadamente treinados para realizar o tratamento de dados em questão. Além disso, a Operadora de Dados Pessoais deverá limitar o acesso aos dados pessoais da Controladora de Dados à equipe que realiza o tratamento relevante, de acordo com o Contrato.

1.5. A Operadora de Dados Pessoais deverá implementar medidas técnicas e organizacionais apropriadas projetadas para proteger a segurança, confidencialidade e integridade dos dados pessoais da Controladora de Dados nos termos do Contrato, incluindo a proteção contra tratamento não autorizado ou ilícito e contra destruição, perda ou alteração acidental ou ilícita, divulgação ou acesso não autorizado aos dados pessoais da Controladora de Dados nos termos do Contrato, de acordo com os requisitos da LGPD [Lei Geral de Proteção de Dados] n. 13.709/2019, com referência específica ao Art. 46. Sem prejuízo ao supracitado, as medidas técnicas e organizacionais apropriadas incluirão, em um nível mínimo, aquelas listadas no Anexo de Segurança da TI, que constitui os requisitos mínimos de segurança identificados pela Controladora de Dados. A conformidade com o Anexo 1 não afeta a obrigação geral da Operadora de Dados Pessoais de implementar medidas de segurança adicionais, se assim consideradas apropriadas com base na melhor prática da indústria.

1.6. A Operadora de Dados Pessoais deverá auxiliar a Controladora de Dados adotando medidas técnicas e organizacionais apropriadas, como e quando necessário, para garantir a proteção dos direitos dos titulares de dados e responder a pedidos de exercício dos direitos dos titulares de dados estabelecidos no Capítulo III da LGPD, sem atrasos indevidos.

1.7. A Operadora de Dados Pessoais não tem autorização de contratar os Subprocessadores para cumprir suas obrigações nos termos do Contrato, salvo mediante consentimento e acordo por escrito entre as partes.

1.8. A Operadora de Dados Pessoais deverá, a qualquer momento, a pedido da Controladora de Dados, ou quando as disposições do Contrato deixarem de ter vigência por qualquer motivo, apagar de forma permanente de seus sistemas, com exceção de quaisquer cópias de backup que a Operadora de Dados Pessoais deve reter para cumprimento das leis ou requisitos regulatórios, desde que essas cópias sejam mantidas confidenciais e seguras, de acordo com o Contrato.

1.9. Se a Operadora de Dados Pessoais violar o presente CTD determinando os objetivos e os meios de tratamento, ela deverá ser considerada uma Controladora de Dados em relação a esse tratamento, para qual deverá assumir responsabilidade.

2. Obrigações e Direitos da Controladora de Dados

2.1. A Controladora de Dados deverá fornecer instruções relacionadas aos métodos e objetivos do tratamento de dados, no início das atividades de tratamento e dados e de tempos em tempos, conforme venha a ser necessário. Todas as instruções deverão estar por escrito e compartilhadas por correspondência ou e-mail.

2.2. A Controladora de Dados deverá ter o direito de obter da Operadora de Dados Pessoais, assim que viável e sem atrasos indevidos, quaisquer informações exigidas pela Autoridade Nacional.

2.3. A Controladora de Dados poderá rescindir o CTD imediatamente entregando um aviso escrito à Operadora de Dados Pessoais, se a Operadora de Dados Pessoais tratar dados pessoais em violação ao CTD ou às leis de privacidade aplicáveis, quando aplicável, dependendo da nacionalidade e do local de contabilização dos clientes.

3. Contatos para questões de proteção de dados

3.1. Para a Controladora de Dados e Operadora de Dados Pessoais: Todas as comunicações relacionadas a questões de proteção de dados deverão ser realizadas aos cuidados de cada Data Protection Officer de cada parte (“Encarregado de Proteção de Dados”)

ANEXO 1: ANEXO DE SEGURANÇA DE TI

A Operadora de Dados Pessoais respeita as medidas de segurança prescritas pela Controladora e adotadas nas instalações onde o tratamento ocorre, de acordo com e para os objetivos da LGPD em especial os Capítulos II e VII.

Em consequência disso, a Operadora de Dados Pessoais deve garantir, principalmente, que respeita as seguintes medidas prescritas pelo Capítulo VII, artigos 46 a 50:

- a pseudonimização e criptografia dos dados pessoais;
- a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência progressivas dos sistemas e serviços de TI de tratamento de dados;
- a capacidade de restaurar a disponibilidade e o acesso a dados pessoais de forma tempestiva, na hipótese de um incidente técnico ou físico;
- um processo para o teste e avaliação regulares da eficácia de medidas técnicas e organizacionais para garantia da segurança do tratamento.

Além disso, a Operadora de Dados Pessoais garante:

- o armazenamento e o arquivamento corretos de dados pessoais comuns e sensíveis nos escritórios em que as operações de tratamento ocorrem;
- a identificação, por nome e por escrito, dos titulares autorizados a tratar dados;
- a restrição de acesso às dependências onde os arquivos estão localizados.

A Operadora de Dados Pessoais deve garantir que estas medidas de segurança sejam suficientes para minimizar os seguintes riscos:

- destruição intencional ou acidental ou perda de dados;
- acesso não autorizado;
- tratamento não autorizado;
- tratamento não conforme com os objetivos das Operações de Tratamento.

A Empresa e o Cliente se reservam ao direito de verificar, a qualquer ponto durante o curso do contrato, a conformidade das ações da Operadora de Dados Pessoais de acordo com as instruções fornecidas; e o direito de auditar as medidas técnicas e organizacionais implementadas pela Operadora de Dados Pessoais para garantir um nível adequado de

segurança dos dados e o tratamento realizado em nome da Empresa e do Cliente. Ao avaliar o nível de segurança adequado garantido pela Operadora de Dados Pessoais, a Empresa e o Cliente consideram os riscos que derivam do tratamento acidental ou ilícito de dados, como destruição, perda, modificação, divulgação ou acesso não autorizado a dados pessoais transmitidos, armazenados ou, em qualquer caso, tratados em seu nome.

1. Medidas de segurança organizacionais

Políticas e Regulamentos do Usuário - A Operadora de Dados Pessoais aplica as políticas e regulamentos detalhados que todos os usuários que acessam os sistemas de informação devem seguir, a fim de garantir um comportamento adequado que respeita os princípios de confidencialidade, disponibilidade e integridade de dados pessoais no uso de sistemas de TI.

Autorização de acesso lógico - A Operadora de Dados Pessoais define os perfis de acesso, de acordo com o princípio de segurança de "menos privilégios" necessários para executar os deveres atribuídos. Os perfis de autorização são identificados e configurados antes do início do tratamento, quanto a fornecer acesso somente aos dados pessoais necessários para executar as operações de tratamento.

Estes perfis são periodicamente revisados para verificar se as condições para os perfis alocados estão mantidas.

Gestão de Mudanças - A Operadora de Dados Pessoais adotou um procedimento especial por qual regula o processo de Gestão de Mudanças em virtude da introdução de quaisquer inovações tecnológicas ou mudanças de sua configuração e estrutura organizacional.

Gestão de Incidentes - A Operadora de Dados Pessoais implementou um procedimento específico de Gestão de Incidentes para garantir a recuperação de operações de serviço normais assim que possível, em caso de interrupção, garantindo que os níveis de serviço acordados sejam mantidos.

A Operadora de Dados Pessoais é responsável por notificar imediatamente a Empresa e o Cliente sobre quaisquer incidentes de segurança relacionados à confidencialidade e integridade dos dados; se o incidente for atribuível às atividades sob a alçada da Operadora de Dados Pessoais, as ações corretivas necessárias para reduzir o risco subsequente também devem ser ativadas.

Violação de Dados - A Operadora de Dados Pessoais implementou um procedimento específico com objetivo de gerenciar eventos e incidentes com impacto potencial sobre os dados pessoais, que define as funções e responsabilidades, o processo de detecção (pressuposto ou confirmado), a aplicação de contramedidas e a resposta e contenção do incidente/violação. Na

medida em que a Operadora de Dados Pessoais é responsável, este procedimento identifica o seguinte, a título de relatório de incidente específico:

- a natureza da violação de dados pessoais, incluindo, quando possível, as categorias e o número aproximado de titulares de dados em questão e as categorias e o número aproximado de registros de dados pessoais em questão;
- as consequências prováveis da violação de dados pessoais;
- as medidas adotadas ou propostas para corrigir a violação de dados pessoais, incluindo, quando apropriado, medidas adotadas para mitigar seus possíveis efeitos adversos;

A Operadora de Dados Pessoais deve notificar imediatamente a Empresa e o Cliente sobre qualquer tratamento ilícito de dados pessoais realizado na assinatura do presente contrato, em sua organização, de forma a permitir que a Empresa e o Cliente notifiquem de forma tempestiva a Autoridade Nacional e o titular de dados sobre a violação de dados pessoais, em casos em que o controlador é responsável por estas obrigações, de acordo com a LGPD em especial o artigo 46.

Treinamento: A Operadora de Dados Pessoais ministra treinamentos regulares sobre o tratamento correto de dados pessoais a seus usuários envolvidos em atividades de assistência técnica.

2. Medidas de segurança técnica

Planejamento de capacidade - A Operadora de Dados Pessoais implementou um processo operacional para a revisão periódica do desempenho e da capacidade dos recursos de TI, organizada com objetivo de garantir níveis de desempenho apropriados aos requisitos e à continuidade do serviço gerenciado. O processo inclui a previsão de requisitos futuros com base nos requisitos de carga de trabalho e armazenamento de dados.

Severidade [Hardening]- Atividades específicas de *hardening* estão em operação, com objetivo de prevenir a ocorrência de incidentes de segurança, minimizando as fraquezas arquitetônicas de sistemas operacionais, aplicativos e dispositivos em rede, considerando - especificamente - a redução de riscos relacionados a vulnerabilidades do sistema, à redução de riscos relacionados ao contexto de aplicação nos sistemas e ao aumento dos níveis de proteção dos serviços prestados por estes sistemas.

Gerenciamento de Fragmentos [Patches] - Um processo específico de gerenciamento de *patches* é gerenciado com objetivo de garantir a atualização constante dos sistemas a fim de prevenir vulnerabilidades e corrigir defeitos.

Dispositivo de Segurança, SDPI [Firewall] - Os dados pessoais são protegidos contra o risco de intrusão, mantidos atualizados de acordo com as melhores tecnologias disponíveis.

Proteção contra Software Nocivo [Malware] - Os sistemas são protegidos contra risco de intrusão e a ação de programas por meio da ativação de ferramentas eletrônicas adequadas, atualizadas regularmente (pelo menos, semestralmente).

As ferramentas antivírus são utilizadas e mantidas constantemente atualizadas.

Segurança da linha de comunicação - Em sua área de responsabilidade, a Operadora de Dados Pessoais adota protocolos de comunicação seguros em conformidade com a tecnologia disponível, de forma a garantir a segurança na transmissão de dados e no processo de autenticação.

Proteção física do Centro de Dados - O acesso físico ao Centro de Dados só é permitido ao pessoal autorizado, de acordo com os métodos regulamentados em um procedimento específico. Quaisquer visitantes ou pessoas externas que precisam de acesso às áreas do Centro de Dados e, quando autorizados para acesso temporário, estarão acompanhados durante toda a visita pelo pessoal com autorização permanente.

O acesso às salas internas onde os sistemas residem está sujeito a medidas de segurança mais rígidas e é registrado em um *log* especial que pode ser consultado por uma equipe supervisora autorizada.

A segurança do perímetro é garantia por sistemas de alarme configurados em relação às características das infraestruturas e por sistemas monitorados de vigilância por vídeo.

As salas internas possuem medidas de segurança ambiental adequadas (sistemas de prevenção contra incêndio, painéis duplos de controle elétrico, sistemas de ar condicionado redundantes, UPS/unidades geradoras que garantem a continuidade do abastecimento de energia aos sistemas, linhas de comunicação redundantes, etc.).

Todos os sistemas e equipamentos técnicos estão sujeitos à manutenção regular e periódica executada por empresas especializadas.

As premissas estão em conformidade com as disposições da Consolidaçao das Leis do Trabalho – CLT, leis complementares e normas regulamentadoras conforme aditadas e complementadas.

Segurança de Rede - Se parte da rede/LAN estiver sob responsabilidade da Operadora de Dados Pessoais, medidas de segregação adequadas também devem ser adotadas para evitar o risco de seus outros clientes ou pessoas não autorizadas acessarem os sistemas ou dados. Além disso, todas as conexões remotas aos sistemas da Empresa e do Cliente e as transmissões de dados devem utilizar protocolos seguros (VPN, SFTP, HTTPS, etc.). Um sistema robusto de autenticação também deve ser utilizado (OTP, tokens, etc.).

Credenciais de autenticação - Os sistemas são apropriadamente configurados para somente permitir acesso às pessoas com credenciais de autenticação, permitindo sua identificação única por meio de um procedimento de autenticação. Elas podem consistir em um código associado a uma palavra-chave (confidencial e de conhecimento exclusivo da pessoa) ou um dispositivo de autenticação detido exclusivamente pela pessoa, possivelmente associada a um código de identificação ou palavra-chave.

Palavra-chave - Em termos das características básicas da palavra-chave, isto é, a obrigação de alterá-la no primeiro acesso, comprimento mínimo, ausência de elementos que podem ser facilmente ligados à pessoa, regras de complexidade, vencimento, histórico, avaliação de força, exibição e arquivamento, ela é gerenciada em conformidade com as melhores práticas. As pessoas a quem as credenciais são atribuídas recebem instruções precisas sobre os métodos de uso para garantir seu sigilo.

Autenticação Forte - As técnicas de autenticação forte devem ser adotadas para garantir o acesso exclusivamente ao pessoal responsável nos seguintes casos: se os dados pessoais relacionados aos riscos aos direitos e liberdades de pessoas físicas e/ou jurídicas forem processados e se as características dos perfis de autorização forem de alto nível (por exemplo, direitos plenos).

Logging - Os sistemas são configurados de forma a permitir o rastreamento de acessos e, quando apropriado, das atividades realizadas, de acordo com os diferentes tipos de usuários técnicos, protegidos por medidas de segurança adequadas que garantem a integridade.

Continuidade dos Negócios - Quando previstas nos instrumentos contratuais, as medidas adequadas devem ser adotadas para garantir a recuperação do acesso aos dados no caso de dano aos dados ou equipamentos eletrônicos, dentro de determinados intervalos, compatíveis com os direitos dos titulares de dados. A fim de garantir o funcionamento correto e a realização correta dos processos de backup em termos de integridade e disponibilidade das cópias criadas, testes específicos de recuperação são realizados com frequência estabelecida em relação à importância dos dados (em geral, trimestralmente).

Se previsto nos instrumentos contratuais, um plano de continuidade dos negócios é implementado e integrado, quando necessário, ao plano de recuperação de desastres. Estes planos garantem a disponibilidade e o acesso aos sistemas, mesmo no caso de eventos negativos significativos que venham a persistir com o tempo. A testagem anual do plano é realizada e os resultados são disponibilizados à Empresa.

Administradores do Sistema - O seguinte é realizado em relação a todos os usuários que operam na qualidade de Administradores do Sistema (AS):

- Atribuição das funções de AS, sujeita à avaliação da experiência, capacidade e confiabilidade das pessoas nomeadas;

- Nomeação escrita do AS, indicando as áreas de operação permitidas com base nos perfis de autorização atribuídos e especificando que sua função não inclui qualquer acesso a dados presentes nos bancos de dados da Empresa e do Cliente e que a integridade dos dados é também um requisito legal;

- Preparo de sistemas apropriados para gravar as atividades do AS. Estes registros devem estar completos, inalteráveis e incluir a possibilidade de verificação de sua integridade, de forma a alcançar o escopo de verificação para qual têm obrigação e proceder com seu armazenamento (um ano);

- Verificações regulares, indicativamente mensalmente, sobre o trabalho do AS, fornecendo um relatório de análise bimestral definido quaisquer operações anormais ou operações que excedem a autorização recebida, e um resumo das atividades realizadas de acordo com um formato acordado com a Empresa e o Cliente;

- Garantir que os PCs utilizados pelo AS estão adequadamente protegidos contra acesso não autorizado no caso de roubo ou perda do PC ou seu disco rígido.

Avaliação de Vulnerabilidade e Teste de Invasão - A Operadora de Dados Pessoais realiza regularmente análises de vulnerabilidade com objetivo de identificar o status de exposição a vulnerabilidades conhecidas, em relação aos ambientes de infraestrutura e aplicação, considerando os sistemas em fase de operação ou desenvolvimento.

Se considerados apropriados em relação aos potenciais riscos identificados, estas verificações são periodicamente suplementadas por Testes de Invasão específicos. Eles envolvem simulações de intrusão que usam cenários diferentes de ataque, com objetivo de verificação do nível de segurança de aplicativos / sistemas / redes através de atividades com objetivo de explorar as vulnerabilidades identificadas para desviar os mecanismos de segurança física / lógica e ganhar acesso a eles.

Os resultados das verificações disponibilizados a pedido da Empresa são precisamente examinados de forma detalhada para identificar e implementar as ações de melhoria necessárias para garantir o alto nível de segurança necessário.

3. Atividades de manutenção e suporte e migração de dados

Atividades de suporte

- A Operadora de Dados Pessoais adotou um procedimento específico que regula a gestão de atividades de suporte com objetivo de garantir a execução somente destas atividades previstas contratualmente, e impedir o tratamento excessivo de dados pessoais controlados pelo Cliente ou pelo Usuário Final. Especificamente, o procedimento regula os seguintes aspectos:

  - ✓ as habilidades e responsabilidades pela ativação dos usuários técnicos que devem executar a atividade e os respectivos médicos de autenticação a serem adotados;

  - ✓ conexão por meio de canais seguros apropriados ao tipo de dados tratados;

  - ✓ os métodos de desativação das credenciais de usuários técnicos no fim das atividades;

  - ✓ o armazenamento de dados exclusivamente pelo tempo estritamente necessário para identificar e resolver um problema e a supressão de qualquer cópia, incluindo quaisquer relatórios eletrônicos ou impressos produzidos;

  - ✓ as responsabilidades relacionadas às atividades de monitoramento em relação às atividades realizadas.

- A Operadora de Dados Pessoais implementou procedimentos operacionais e métodos de autenticação específicos para garantir que as atividades realizadas podem sempre ser atribuídas, mesmo após o ocorrido, a uma pessoa específica, unicamente identificada e autorizada a realizar a atividade.

- A fim de resolver um problema, sempre que for necessário adquirir o banco de dados do Cliente para realizar atividades analíticas, sujeitas à autorização formal do Cliente, adquiridas e arquivadas nos registros, a Operadora de Dados Pessoais:

  - ✓ usa exclusivamente canais seguros e protegidos, em conformidade com a tecnologia disponível;

  - ✓ em caso de dados sensíveis, conforme definido no Art. 11 da LGPD ou - em qualquer caso - dados que apresentam potencialmente riscos em relação aos direitos e liberdades de pessoas físicas, adquire o banco de dados somente após sua criptografia, aplicando algoritmos adequados para garantir um nível adequado de proteção mesmo que, por qualquer motivo, os dados entrem em posse de titulares não autorizados a acessá-los;

- ✓ restaura o banco de dados em um ambiente dedicado, equipado com as medidas de segurança adequadas para garantir sua confidencialidade e, em qualquer caso, não menos do que aquelas implementadas pelo Cliente ao utilizar os dados no ambiente de produção;

- ✓ só permite pessoal responsável por resolver o problema de acesso aos dados;

- ✓ armazena os dados adquiridos somente pelo tempo necessário para identificar e resolver o problema, apagando o banco de dados e os relatórios eletrônicos ou impressos produzidos no fim das atividades.

Migração de dados

Considerando um tempo decorrido razoavelmente maior, as medidas de segurança aplicadas pela Operadora de Dados Pessoais em relação às atividades de migração de dados são semelhantes àquelas relacionadas à aquisição do banco de dados para a resolução de problemas. Em essência, elas incluem:

- o uso de canais seguros e protegidos para transmissão de dados, em conformidade com a tecnologia disponível.

- em caso de dados sensíveis, conforme definido no Art. 11 da LGPD ou - em qualquer caso - dados que apresentam potencialmente riscos em relação aos direitos e liberdades de pessoas físicas, a transmissão do banco de dados só é realizada após sua criptografia, aplicando algoritmos adequados para garantir um nível adequado de proteção mesmo que, por qualquer motivo, os bancos de dados entrem em posse de titulares não autorizados a acessá-los.

- o uso dos bancos de dados contendo dados reais em um ambiente dedicado, equipado com medidas de segurança adequadas para garantir sua confidencialidade e, em qualquer caso, não menos do que aquelas implementadas pelo Cliente ao utilizar os dados no ambiente de produção. Especificamente, isto se refere ao ambiente preparado para o teste de atividades estendidas, por definição, a todo o banco de dados.

- configuração dos perfis de acesso a esses ambientes somente para o pessoal responsável por gerenciar as atividades de migração, incluindo o teste e a verificação. Se necessário, estes perfis também são estendidos ao pessoal do Cliente. Quando apropriado, o acesso remoto sempre ocorre com uso de canais seguros (HTTPS ou TLS).

- execução do procedimento que testa atividades utilizando os dados pessoais na medida em que quantitativamente necessário para verificar as funções implementadas.

- armazenamento de dados exclusivamente até a conclusão bem sucedida das atividades de verificação e a consequente entrega, aprovação e aceite do Cliente.

Em geral, em relação ao uso dos dados do Cliente para atividades de manutenção, suporte ou migração de dados, a Operadora de Dados Pessoais adota uma política de conduta específica, disponibilizada ao pessoal da Empresa e do Cliente.

ANEXO V - POLÍTICA DE RESPOSTA A INCIDENTES RELACIONADOS A DADOS PESSOAIS

Esta Política tem como objetivo preparar o CONTROLADOR e seus agentes de tratamento terceirizados para lidar com a gestão de um incidente de segurança garantindo que responda de forma mais rápida, organizada e eficiente ao evento, minimizando suas consequências para todos os envolvidos. O nível da resposta dependerá do tipo de dados e da complexidade do tratamento aplicado. Antes de mais nada, é necessário definir o que é um incidente. De maneira geral, um incidente é uma situação inesperada, capaz de alterar a ordem normal das coisas e, no caso da proteção de dados, colocar em risco dados pessoais dos indivíduos que se relacionam com a Instituição. O *National Institute of Standards and Technology (NIT),* define um incidente de segurança como uma violação ou ameaça de violação da política de segurança computacional, política de uso aceitável ou padrões de prática de segurança. De acordo com o artigo 46 da Lei Geral de Proteção de Dados (LGPD), os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

Seguindo o disposto no artigo 48 da LGPD, é obrigação do controlador comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Devendo esta comunicação ser feita em prazo razoável, conforme definição da autoridade nacional, tendo em seu conteúdo, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos; A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata;
- As medidas que foram ou que estão sendo tomadas para reverter ou mitigar os efeitos do prejuízo.

Com base no exposto, a Política de Resposta a Incidentes do CONTROLADOR, aplicável inclusive a qualquer agente de tratamento que trate dados pessoais relacionados ao CONTROLADOR, inclusive terceiros e parceiros do CONTROLADOR, seguirá as etapas ilustradas na figura abaixo e descritas na sequência:

Figura 1: Etapas da Resposta a Incidentes.

1. PLANEJAMENTO

Consiste em identificar, prever e descrever possíveis situações de violação de dados, bem como as respectivas ações que deverão ser tomadas, os prazos e as formas de registro, garantindo que em situações reais se tenha um plano de ação previamente traçado. O planejamento deverá conter, no mínimo:

a. a previsão de possíveis situações de sinistros bem como as formas de monitoramento e a ação que deverá ser tomada em caso de sua ocorrência;

b. a definição da área que deverá ser informada em situação de ocorrência do sinistro e como reportar;

c. o detalhamento das ações necessárias deve levar em conta a criticidade do evento.

Exemplo de detalhamento de incidente:

Incidente	Criticidade	Categoria Dado Digital ou Físico	Como é monitorado	A quem reportar	Ações para contenção	Ações para erradicação	Ações de Recuperação

2. IDENTIFICAÇÃO

Deve-se definir os critérios para detectar, identificar e registrar as situações de incidentes e descrever os recursos utilizados para a identificação de alertas de segurança e acionamento das equipes responsáveis para que sejam tomadas as devidas providências. Devem ser avaliadas todas as possíveis fontes capazes de representar uma ameaça à proteção de dados. Abaixo, algumas situações que devem ser consideradas suspeitas:

- Recebimento de e-mails com caracteres e/ou arquivos anexos suspeitos;
- Comportamento inadequado de dispositivos;
- Problema no acesso a determinados arquivos ou serviços;
- Roubo de dispositivos de armazenamento ou computadores com informações;
- Alerta de software antivírus;
- Consumo excessivo e repentino de memória em servidores ou computadores;
- Tráfego de rede incomum;
- Conexões bloqueadas por firewall;

Análise dos logs de tentativas de acesso não autorizado aos servidores. Situações de não cumprimento dos procedimentos internos também podem oferecer riscos à segurança dos dados pessoais, deste modo, a observação da Cartilha de Boas Práticas é de extrema importância. Todos os colaboradores e parceiros da Instituição são responsáveis por reportar qualquer tipo de eventos e fragilidades, que possam causar danos à segurança da informação. A notificação deve ser registrada por e-mail ao Encarregado de Proteção de Dados.

2.1 CATEGORIAS DA VIOLAÇÃO DE SEGURANÇA

A violação de segurança será classificada dentre as categorias citadas a seguir:

a. Material: quando o incidente envolve dados armazenados em dispositivos físicos. Exemplos: perda de portadores de dados, pastas de arquivos perdidas, smartphones perdidos, etc.

b. Verbal: quando há vazamento de dados de forma verbal, seja por indiscrição (comentários acerca de dados pessoais que são percebidos por terceiros e utilizados em má-fé) ou de forma intencional, repassando indevidamente informações sigilosas.

c. Ciberespaço: quando o incidente está relacionado à Tecnologia da Informação. Nessa categoria enquadram-se o hackeamento, mau gerenciamento de patches, codificação incorreta, medidas de segurança insuficientes, etc.

2.2 AVALIAÇÃO DA CRITICIDADE DE SEGURANÇA

Alguns fatores serão determinantes na definição da criticidade de um incidente:

I. A categoria da criticidade: de maneira genérica, o incidente será classificado em uma das categorias abaixo:

a. Risco Baixo: classificação utilizada quando o incidente de segurança de dados afetar apenas dados pessoais, não incluído o número do CPF;

b. Risco Moderado: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF, e/ou pelo menos um dado sensível, não incluído raça, religião, nome social e dados de saúde;

c. Risco Alto: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF e/ou mais que um dado sensível, incluindo raça, religião, nome social e dados de saúde.

II. Dados legíveis/ilegíveis: dados protegidos por algum sistema de pseudonimização (criptografia, por exemplo).

III. Volume de dados pessoais: expresso em quantidade de registros, arquivos, documentos e/ou em períodos de tempo (uma semana, um ano, etc.).

IV. Facilidade de identificação de indivíduos: facilidade com que se pode deduzir a identidade das pessoas a partir dos dados envolvidos no incidente.

V. Indivíduos com características especiais: se o incidente afeta pessoas com características ou necessidades especiais.

VI. Número de indivíduos afetados: dentro de uma determinada escala, por exemplo, mais de 100 indivíduos.

3. CONTENÇÃO

Após um incidente ser identificado como uma violação de segurança, o mesmo deverá ser contido para evitar que outros sistemas sejam afetados ou que ocasionem danos maiores, deve ser previsto ações para a contenção de curto prazo, backup do sistema e contenção a longo prazo. Durante a contenção, deve haver o registro do incidente e das medidas de contenção que foram adotadas, evitando ao máximo a perda de evidências e as provas do ocorrido. É importante lembrar da necessidade de trabalho colaborativo de toda a Instituição, sobretudo dos membros destacados a seguir:

Figura 2: Fluxo da resposta a Incidentes.

Responsável pelo tratamento de dados da área afetada pelo incidente: a partir do momento que foi identificado um possível incidente de segurança de dados, a área responsável pela categoria de dados deve imediatamente informar o encarregado de dados para iniciar o processo de contenção.

- Operador: os operadores de dados, assim como os colaboradores internos, têm a responsabilidade de informar a ocorrência de incidente de segurança ao encarregado de dados, imediatamente.
- Encarregado da Proteção de Dados: após ser informado, o encarregado de proteção de dados deverá avaliar a existência do plano de ação para tal incidente e iniciá-lo, e caso identifique o fato concreto de vazamento de dados pessoais, preencher o documento de Comunicação de Incidente de Segurança, para notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.
- Procuradoria Jurídica: deve ser comunicada no intuito de auxiliar no processo de comunicação à ANPD e titulares de dados e tomar as medidas jurídicas cabíveis.
- Responsável da área de Tecnologia da Informação: será comunicado sempre que o incidente for relacionado a segurança da informação e que seja necessário medidas técnicas de tecnologia.
- Administração do CONTROLADOR: deve validar as medidas propostas no Plano de Respostas a Incidentes e oferecer subsídios para que as mesmas sejam efetivamente cumpridas.

4. ERRADICAÇÃO

Após a ameaça ter sido contida, é necessário proceder com a sua remoção e a restauração dos sistemas que foram afetados, de modo que voltem a operar em sua normalidade.

5. RECUPERAÇÃO

Os sistemas afetados são restabelecidos e voltam a operar em ambiente de produção. É necessário definir as ações que devem ser tomadas para que o sistema volte a sua normalidade. Deve ser realizada uma varredura para identificar as perdas ocorridas e como recuperar o que foi perdido.

6. LIÇÕES APRENDIDAS

É fundamental que os mesmos erros não voltem a acontecer. Assim, é necessário que os incidentes sejam documentados, especificando quais foram os procedimentos de respostas utilizadas para contorná-los, de forma a manter um histórico das ocorrências e das ações tomadas.