GUIA DE PROTEÇÃO DE DADOS PESSOAIS

RECURSOS HUMANOS

OUTUBRO, 2020

FICHA TÉCNICA

Guia de Proteção de Dados Pessoais – Recursos Humanos
Versão 1.0 - Outubro, 2020

PROJETO DE CONFORMIDADE À LEI DE PROTEÇÃO DE DADOS PESSOAIS

Diretoria de Controles Internos - DCI

Maria Alice da Justa Lemos - Diretora de Controles Internos

Centro de Ensino e Pesquisa em Inovação – CEPI (FGV Direito SP)

Coordenação Técnica

Alexandre Pacheco da Silva

Coordenação Executiva

Victor Nóbrega Luccas

Equipe de Pesquisadores

Fábio Ferraz de Almeida
Fabrício Vasconcelos Gomes
Fernando Issao Ninomiya
Laurianne-Marie Schippers
Lívia Pazianotto Torres
Maria Cecilia Oliveira Gomes
Marília Papaléo Gagliardi
Jordan Vinícius de Oliveira
Thaís Duarte Zappelini

Pesquisadores responsáveis por este Guia

Fabrício Vasconcelos Gomes
Marília Papaléo Gagliardi

Gomes, Fabrício Vasconcelos.
Guia de proteção de dados pessoais : recursos humanos / Fabrício Vasconcelos Gomes e Marília Papaléo Gagliardi. - São Paulo : CEPI-FGV Direito SP, 2020.
6v. - (Guia de proteção de dados pessoais ; 6)

Inclui bibliografia.
ISBN: 978-65-87355-25-2

1. Direito à privacidade. 2. Proteção de dados - Brasil. 3. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 4. Recursos humanos. I. Gagliardi, Marília Papaléo. II. Centro de Ensino e Pesquisa em Inovação. III. Fundação Getulio Vargas. IV. Título.

CDU 342.721(81)

Ficha catalográfica elaborada por: Cristiane de Oliveira CRB SP-008061/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

SUMÁRIO

1. CONTEXTUALIZAÇÃO

O presente Guia faz parte da série de documentos da FGV intitulada **"Orientações para a Governança de Dados da FGV"** e tem como objetivo fornecer orientações sobre como gerenciar as diversas atividades e operações de tratamento de dados. Este Guia é um dos frutos do projeto de adequação da FGV em relação a Lei Geral de Proteção de Dados (**LGPD**) e outras leis setoriais sobre o tema.

A Fundação Getulio Vargas consciente da importância e da necessidade de adequar as suas operações de tratamento de dados pessoais a uma nova e ampla regulação sobre o tema, no caso, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – "**LGPD**"), aprovada em agosto de 2018, deu início em maio de 2019 ao seu processo de conformidade. Considerando ainda, que em maio de 2018 entrou em vigor o *General Data Protection Regulation* (Regulation EU 2016/679 – "**GDPR**") e, que este possui pontos de contato com as atividades da FGV na União Europeia (UE), foi decidido que o processo de conformidade regulatória também abarcaria este regulamento além de outras leis setoriais de proteção de dados brasileiras.

A **LGPD** é uma lei transversal, que perpassa por diferentes agentes econômicos no Brasil, como a academia, setor privado, setor público e terceiro setor. Entre os agentes regulados, a FGV se situa no setor acadêmico como uma Instituição de Ensino Superior (IES), abrangendo por esse motivo, uma série de particularidades nos tratamentos de dados pessoais realizados em sua estrutura. Particularmente, a FGV precisa atender às obrigações legais específicas de IES previstas pelo MEC e outras entidades, as quais muitas vezes possuem sinergia com o campo da proteção de dados, devido a particularidades no tratamento de dados do setor educacional, como por exemplo, a necessidade de guarda permanente de históricos escolares, provas, etc.

Considerando que a FGV é uma IES e, portanto, depositária de um grande volume de dados de caráter pessoal coletados em pesquisas científicas e na administração do ensino, por meio de fontes como cadastros de matrícula, históricos escolares, cadastros de professores e funcionários administrativos, entre outros, decidiu-se pela necessidade de desenvolver um projeto para cumprir com os objetivos de sua conformidade regulatória frente às leis de proteção de dados, denominado **Projeto Presidência - Implantação do Programa de Conformidade: Leis de Proteção de Dados Pessoais ("Projeto")**.

Dessa forma, o Projeto visa, primeiramente, a realizar um levantamento das práticas de tratamento de dados pessoais em toda a FGV. Considerando seu histórico, sua dimensão e suas diferentes frentes de atuação, o Projeto tem o objetivo de viabilizar uma análise completa, levando em consideração as distintas particularidades envolvidas em cada uma das atividades desempenhadas pela FGV. O Projeto tem como objetivo também desenvolver metodologias e mecanismos de análise para elaboração de Relatórios de Impacto à Proteção de Dados que visem a contribuir com a construção de uma cultura de proteção de dados na FGV e nas demais IES no País.

Como resultado desse trabalho, busca-se desenvolver: (i) a conformidade da FGV ao novo contexto regulatório de proteção de dados da **LGPD** e, subsidiariamente, àquele estabelecido pela **GDPR**; e (ii) estabelecer um protocolo de conformidade ao novo marco legal de proteção de dados pessoais em IES, com potencial de disseminação e replicação por outras instituições e de influência de agentes governamentais e outros atores privados.

O processo de conformidade envolve um trabalho de interpretação da lei para definição das obrigações legais, diagnóstico dos fatos pertinentes e relevantes para a sua aplicação e levantamento de fluxos e processos que contribuem ou não para que os fatos estejam de acordo com o documento legal.

2. DEFINIÇÕES

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.

2.1. 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 da FGV para com a LGPD, serve de base para que todos os colaboradores que realizem a função de RH em Instituições de Educação Superior (IES) ou suas Mantenedoras, 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 das IES 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 das IES com as práticas previstas na LGPD;

(b) Descrever as regras comportamentais a serem seguidas na condução das atividades desenvolvidas nas IES, 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;

Os demais documentos do Programa de Conformidade da FGV para com a LGPD que se relacionam com este Guia são:

(i) Política de Privacidade e Proteção de Dados Pessoais FGV;

(ii) Guia de Proteção de Dados Pessoais: Pesquisa;

(iii) Guia de Proteção de Dados Pessoais: Crianças e Adolescentes.

5. POR QUE É RELEVANTE A PROTEÇÃO DE DADOS NA UNIDADE DE RECURSOS HUMANOS DAS IES?

As áreas de Recursos Humanos das IES são responsáveis pelo tratamento de uma série de dados pessoais de diferentes tipos de colaboradores ligados a essas instituições. 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) em Instituições de ensino superior (IES) ou suas mantenedoras; o terceiro (seção 7) destinado a esclarecer como devem ser tratados os dados daqueles colaboradores efetivados junto às IES ; e o quarto (seção 8) destinado a identificar como deve ser o tratamento dos dados pessoais dos colaboradores após seu desligamento de IES.

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 uma IES, 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). Uma IES pode trabalhar com diferentes regimes de colaboração, sejam vínculos de emprego, de prestação de serviço ou outros tipos, representados, ilustrativamente, no quadro abaixo. Essas colaborações, note-se, nem sempre são gerenciadas por um único órgão dentro da IES, 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 pelo corpo docente de uma Faculdade da IES.

As orientações deste Guia se aplicam às situações em que o vínculo entre colaboradores e as IES são constituídos e administrados por uma área dedicada, a Unidade de RH, 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 em uma IES.

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 às IES. 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 as IES em sua área 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) A Portaria do Acervo Acadêmico Digital estabelecida pelo MEC. Esta estabelece o "Ciclo de Vida" para diversos documentos que contêm dados pessoais de Colaboradores, além de

determinar a obrigatoriedade de algumas formas de tratamento.

(iii) Nesses casos, esta continua vigendo de acordo com suas disposições sobre o tempo de descarte e eliminação do dado pessoal coletado. Isso porque já existe 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.

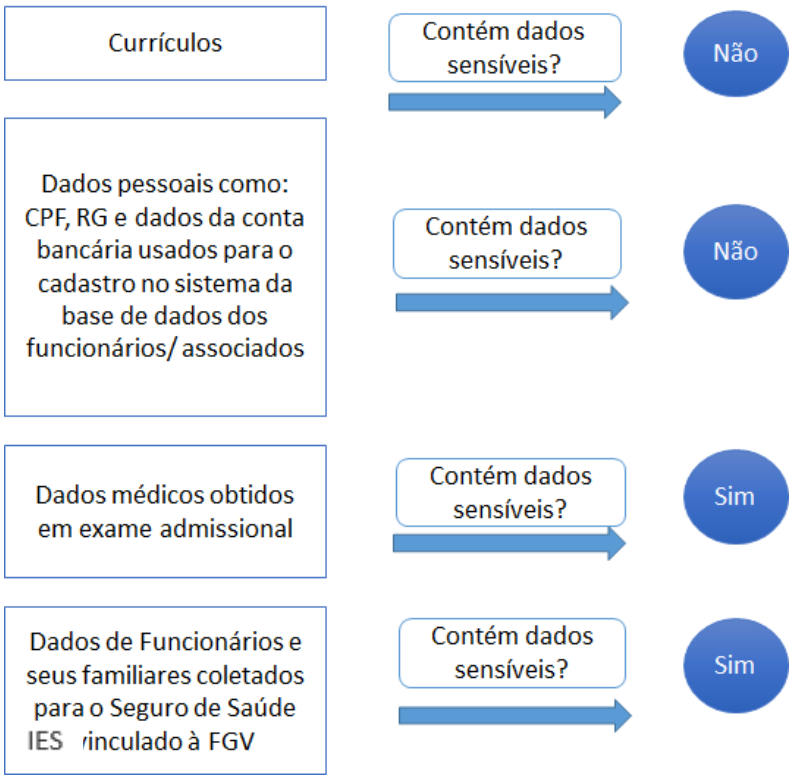
Nessas hipóteses, o procedimento de ciclo de vida tem de ser avaliado caso a caso, identificando a justificativa para a coleta e preservação do dado:

(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 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 IES. A seguir, exemplos de documentos e dados pessoais sensíveis ou não:



Esses exemplos são exemplificativos. 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.

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 IES, 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 da IES 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 ados 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 DE 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 Jurídico da IES.

- **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? 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?

- **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?

Como regra geral, a resposta é negativa, nas três hipóteses elencadas.

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 Jurídico da IES, 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 da IES, 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.

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

[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.

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 através de 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, 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).

(iii) 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 IES 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 na mesma IES, 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 IES 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 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 da IES, 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 da IES, 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, 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 pela IES com a citada finalidade cause danos a terceiros, por descumprimento da LGPD, e a mesma IES 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 da IES 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 adstritos 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 IES, 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 IES 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; e
- ✓ 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. É o caso, por exemplo, de currículo no formato da plataforma Lattes, cópias de diplomas de mestrado ou doutorado, quando o colaborador for professor. Estes documentos são necessários para fins de cumprimento de regulação do ensino superior, como verificação e comprovação de titulação do corpo docente.

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

[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>.

(ii) Armazenamento

O tempo de armazenamento dos dados tratados deve ser equivalente ao tempo de vigência do vínculo estabelecido entre o colaborador e a IES, 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 IES. Nesse sentido, tem-se que muitas vezes, o compartilhamento, ao menos interno à IES, 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 IES. Ainda, pode ser necessário que exista o compartilhamento com a unidade competente dentro da IES, para que seja feito um crachá para o colaborador.

O compartilhamento também pode ser feito externamente à IES, 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, consoante o Guia Sobre Compartilhamentos, 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 IES 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 informa-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 IES. 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 IES.

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 IES, 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 das IES. 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 IES 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 IES e seus colaboradores. Por exemplo, registros de entrada e saída de prédios, avaliações de professores feitas por alunos, 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 IES 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 da IES (mapa de lugares).

Os dados pessoais, portanto, só devem ser mantidos após o fim do vínculo entre colaborador e IES: (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 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 IES.

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 IES e

[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.

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 IES. 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 IES para um processo de admissão, situação em que ele estaria pleiteando o compartilhamento externo de dados de colaboradores de tal IES.

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 IES 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 IES 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 IES e uma terceira empresa, que efetivamente concede o benefício (geralmente é o caso de planos de saúde, por exemplo).

Nesses casos, a IES 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 IES, 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 IES 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 IES 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 das IES.

Nesse sentido, após o término do vínculo estabelecido entre o colaborador e a IES, 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 IES, situação em que a mesma IES 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, 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 IES.

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 IES.

- **Dados relativos ao registro da história da instituição**

Uma IES sempre 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 instituição, como grandes pesquisadores, professores 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. Para maiores detalhes sobre essa hipótese, recomenda-se a consulta ao *Guia de Proteção de Dados Pessoais: Pesquisa*.

Por fim, considera-se a hipótese de a IES ter a pretensão apenas de ter uma estimativa relativa à capacitação de seus colaboradores. Por exemplo, a instituição pode ter como objetivo apenas saber quanto professor doutores em direito empresarial passaram por sua faculdade de direito. 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.

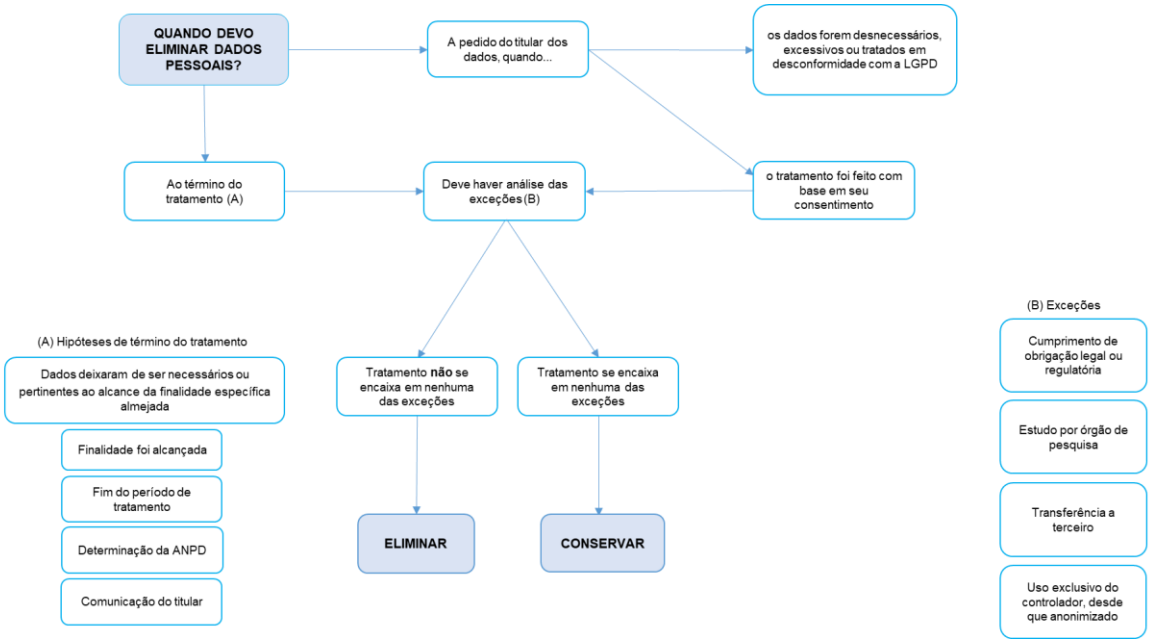
Existe, por fim, a eliminação decorrente do término do tratamento (iii). Nesses casos, quando inexistir a necessidade de guarda dos documentos, consoante dispostos nas regras dispostas nos tópicos acima, estes devem ser eliminados.

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 IES 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 IES 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.

REFERÊNCIAS

BRASIL. **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 ago. 2020.

PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. **GENERAL DATA PROTECTION REGULATION** – EU 2016/679. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt>. Acesso em: 12 jun. 2020.

APÊNDICE 1: MODELO DE TERMO DE CIÊNCIA E CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS DE MENOR DE 16 (DEZESSEIS) ANOS

Trata-se de termo de consentimento do(a) responsável legal pelo(a) [titular de dados pessoais, ex. estudante] que não atingiu os 16 (dezesseis) anos completos, autorizando a coleta os dados do menor para [descrição da finalidade e indicação do controlador].

(I) IDENTIFICAÇÃO DO(A) TITULAR MENOR E DE SEU/SUA RESPONSÁVEL LEGAL (nome e CPF do menor com idade entre 12 anos completos e 16 anos incompletos e de seu responsável legal):

[Preenchimento pelo responsável]

- Nome **Estudante:** _____

- CPF **Estudante**: _____

- Nome **Responsável Legal:** _____

- CPF **Responsável Legal**:_____

(II) AGENTES DE TRATAMENTO [entes públicos e privados responsáveis por usar os dados pessoais do menor devem estar discriminados]

(a) CONTROLADOR 1 (nome, representante e endereço da unidade/subunidade)

[Digitado pelo colaborador da unidade/subunidade. Ex. Secretaria]

_____
_____

_____

(b) CONTROLADOR 2 (nome, CNPJ, representante e endereço)

[Digitado pelo colaborador da unidade/subunidade. Ex. Secretaria]

_____
_____

_____

(III) REFERÊNCIA CONTRATUAL E VALIDADE DAS OPERAÇÕES DE TRATAMENTO (contrato ou acordo de cooperação que vincula os agentes controladores para tratar os dados do(a) menor titular):

- As operações de tratamento de dados pessoais do(a) titular a quem este termo de consentimento se refere têm por base a execução de Acordo X celebrado entre o Controlador X e o Controlador Y em ____/____/_____ e durarão enquanto este Acordo for válido;

[Digitado pelo colaborador da unidade/subunidade. Indicar Acordo, ex. Acordo de Cooperação, se houver]

(IV) DADOS PESSOAIS DO(A) TITULAR OBJETO DE TRATAMENTO -o(a) responsável legal pelo menor de 16 anos está ciente de que os seguintes dados pertencentes ao menor serão tratados pelos Controladores 1, 2 e 3 no âmbito [dos serviços X, Y,Z]

- Ex. nome do(a) responsável legal; nome completo do(a) titular; endereço de e-mail; sexo; data de nascimento; número de CPF; número de RG; grau de escolaridade; nome da instituição a que está vinculado; dados de acesso (IP, nome de usuário(a), e-mail, senha, data e hora de acesso).

(V) FINALIDADE(S) DO TRATAMENTO DE DADOS (objetivo para o qual os dados pessoais do menor de 16 anos serão tratados pelos controladores 1, 2 e 3):

- EX. finalidade de oferecimento de serviços de aperfeiçoamento educacional do ensino-aprendizagem.

- Ex. A IES poderá utilizar os dados para viabilizar pesquisas acadêmicas e/ou aplicadas. Estou ciente de que, pelo motivo destes dados serem anonimizados ou não identificados, o seu uso pela IES é plenamente possível sem a necessidade de meu consentimento, como dispõe a Lei nº 13.709/2018.

(VI) COMPARTILHAMENTO (ciência de que os dados do menor de 16 anos poderão ser compartilhados com os seguintes entes)

[Destacar todos os compartilhamentos, inclusive com entes públicos.]

- O responsável pelo titular menor de 16 anos autoriza que os dados listados no item "IV" sejam compartilhados entre os controladores 1, 2 e 3 para [finalidade do compartilhamento].

(VII) SEGURANÇA DOS DADOS (expedientes de proteção e conservação dos dados pessoais a serem seguidos pelos agentes de tratamento)

- Ex. os dados do(a) titular serão inseridos na Plataforma X por meio da uma Interface Y, disponibilizada para este fim pela IES, a qual deverá ser acessada pela via de chaves de identificação e código de autenticação de responsabilidade das controladoras 1 e 2. A IES envidará todos os esforços para promover a segurança da informação dos dados inseridos na Plataforma, mas é de responsabilidade do(a) usuário(a) proteger suas credenciais de login e senha contra o acesso indevido por terceiros, bem como alterá-las quando solicitado por política de segurança.

(VIII) DIREITOS DO(A) TITULAR (direitos do titular em face das controladoras 1, 2 e 3)

- A partir do momento em que entrar em vigência a Lei 13.709/2018, o(a) titular poderá, por intermédio de seu/sua representante legal, exercer todo e qualquer direito assegurado nesta lei, como: (a) requisitar a confirmação do tratamento; (b) requisitar o acesso aos dados; (c) requisitar a correção dos dados; (d) requisitar a anonimização, o bloqueio ou a eliminação dos dados desnecessários ou excessivos ou, ainda, tratados em desconformidade com a Lei Geral de Dados Pessoais, Lei 13.709/2018; (e) requisitar a portabilidade dos dados, observado o segredo industrial ou comercial; (f) requisitar a eliminação dos dados, ressalvadas as hipóteses de cumprimento de obrigação legal ou de execução de contrato; (g) requisitar informação acerca das entidades públicas e privadas para as quais houve compartilhamento dos dados; (h) a informações acerca da possibilidade de não fornecimento do consentimento, sendo a consequência da oposição à finalidade do item "V" deste termo a impossibilidade de uso dos serviços; (i) requisitar a revogação do consentimento para o tratamento, observada a consequência do item "h";

(IX) DO CONSENTIMENTO (concordância livre, informada e inequívoca, por parte do responsável legal pelo menor de 16 anos, para o tratamento dos dados do representado):

- Na qualidade de responsável legal pelo estudante menor de 16 (dezesseis) anos identificado na cláusula "I", manifesto o meu consentimento livre, informado e inequívoco para que os controladores descritos na cláusula "II" procedam ao tratamento dos dados pessoais listados na cláusula "IV", em atenção à finalidade na cláusula "V" e em observância aos demais componentes deste Termo de Ciência e Consentimento.

_____ (local), _____ de _____ de 20xx.

_____

(Pai, Mãe ou Responsável Legal pelo Titular do dado)

APÊNDICE 2: TRECHO TRADUZIDO DO POSICIONAMENTO DA ICO SOBRE O CONCEITO DE "ESFORÇOS RAZOÁVEIS"

Abaixo apresentamos trecho traduzido do posicionamento da *Information Comissioner's Office* (ICO) em relação ao conceito de "esforços razoáveis" para obter a obtenção do consentimento dos pais ou responsáveis legais de crianças e adolescentes, via tecnologias disponíveis.[4]

O que significa "razoáveis esforços"?

Isso varia a depender dos riscos intrínsecos envolvidos e da tecnologia que esteja disponível.

Por exemplo, você pode requerer um endereço de e-mail para uma criança que queira se inscrever na newsletter de uma banda por um website. Na medida em que você apenas utilizará o e-mail para enviar as newsletters requeridas, você pode avaliar que os riscos envolvidos em coletar essa informação são pequenos. Um esforço razoável nessas circunstâncias deve, portanto, envolver simplesmente requerer via declaração que o usuário possui a idade necessária para prover o seu consentimento ou uma declaração de consentimento e responsabilidade de seus pais, via checkbox ou confirmação por e-mail. Você pode considerar, assim, que quaisquer requisitos adicionais não são razoáveis (ou práticos de serem implementados) e de que estes simples passos são suficientes, dado o baixo risco para a criança na operação de tratamento proposta.

Entretanto, se o seu serviço informacional [ISS: Information Society Service][5] viabiliza, por exemplo, que os usuários menores postem dados pessoais pela via de uma sala de chat não monitorada, torna-se mais arriscado permitir que crianças participem. Você deve, portanto, adotar meios mais delimitados para verificar o consentimento que você obteve. Por exemplo, você pode implementar um serviço de verificação de terceiro – para verificar que o usuário possui a idade mínima requerida para prover o seu consentimento, ou checar a identidade da pessoa requerendo a responsabilidade dos pais e a confirmação do status de vínculo entre esse responsável e a criança.

A necessidade implícita de verificar a idade levanta o problema de como você fará isso remotamente e por meios amigáveis para coletar elementos identificadores essenciais [hard identifiers], como o passaporte escaneado ou os detalhes de cartão de crédito. Ao mesmo tempo, coletar informações excessivas indica uma prática desconforme à proteção de dados por design, como requerido pela GDPR. Há, ainda, o desafio adicional de que no Reino Unido usuários de 13 a 17 anos possuem um espectro mais limitado de documentos de identificação disponíveis, do que se comparado a adultos (tradução livre).

[4] INFORMATION COMISSIONER'S OFFICE. *Guide to the General Data Protection Regulation.* Tradução livre por Jordan Vinícius de Oliveira. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-are-the-rules-about-an-iss-and-consent/>. Acesso em: 30 abr. 2020.

[5] ISS é qualquer serviço de tratamento de dados pessoais fornecido por meio informacional, como plataformas digitais, chats, jogos e outros.

FGV DCI

DIRETORIA DE
CONTROLES INTERNOS