GUIA DE BOAS PRÁTICAS DE LGPD PARA O SISTEMA INDÚSTRIA

IEL
Instituto Euvaldo Lodi
PELO FUTURO DA INDÚSTRIA

SENAI
Serviço Nacional de Aprendizagem Industrial
PELO FUTURO DO TRABALHO

SESI
Serviço Social da Indústria
PELO FUTURO DO TRABALHO

CNI
Confederação Nacional da Indústria
PELO FUTURO DA INDÚSTRIA

GUIA DE BOAS PRÁTICAS DE LGPD PARA O SISTEMA INDÚSTRIA

GUIA DE BOAS PRÁTICAS DE LGPD PARA O SISTEMA INDÚSTRIA

IEL
Instituto Euvaldo Lodi
PELO FUTURO DA INDÚSTRIA

SENAI
Serviço Nacional de Aprendizagem Industrial
PELO FUTURO DO TRABALHO

SESI
Serviço Social da Indústria
PELO FUTURO DO TRABALHO

CNI
Confederação Nacional da Indústria
PELO FUTURO DA INDÚSTRIA

CNI
Diretoria Jurídica - DJ

FICHA CATALOGRÁFICA

C748g

Confederação Nacional da Indústria.
Guia de boas práticas de LGPD para o Sistema Indústria / Confederação Nacional da Indústria. – Brasília : CNI, 2023.

167 p. : il.

1.LGPD. 2. Tratamento de Dados. 3. Segurança da Informação. I. Título.

CDU: 342.721(094.5)

CNI
Confederação Nacional da Indústria
Sede
Setor Bancário Norte
Quadra 1 – Bloco C
Edifício Roberto Simonsen
70040-903 – Brasília – DF
Tel.: (61) 3317-9000
Fax: (61) 3317-9994
http://www.portaldaindustria.com.br/cni/

Serviço de Atendimento ao Cliente - SAC
Tels.: (61) 3317-9989/3317-9992
sac@cni.com.br

SUMÁRIO

APRESENTAÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), estabeleceu uma nova realidade, a que todas as pessoas físicas e jurídicas devem se submeter para o armazenamento e para a utilização dos dados pessoais.

Numa época em que a economia e a vida das pessoas estão cadenciadas pela velocidade do mundo digital, o tratamento de dados é crucial para a tomada de decisão das instituições.

O tratamento dos dados pessoais está na base do desenvolvimento da Indústria 4.0, nome conferido à quarta revolução industrial, que tem como pilar a digitalização de processos, da produção e dos produtos. Com a utilização apropriada das informações, espera-se aumentar a produtividade, diminuir os custos de produção e aperfeiçoar a segurança da informação.

Nesse sentido, a LGPD se revela fundamental para disciplinar o uso dos dados pessoais com transparência e respeito à liberdade e à privacidade dos indivíduos, trazendo segurança jurídica e reduzindo a possibilidade de conflitos.

Certamente, as instituições precisam adaptar os seus modelos de gestão ao imenso volume de informações e à incalculável velocidade com que são geradas em tempo real. Isso demanda investimentos e, em certos casos, mudança de cultura.

Ciente desse desafio e da importância do tema, que tem inevitável impacto nas atividades que realizam, a Confederação Nacional da Indústria (CNI), os Departamentos Nacionais do Serviço Social da Indústria (SESI/DN) e do Serviço Nacional de Aprendizagem Industrial (SENAI/DN), e o Instituto Euvaldo Lodi Núcleo Central (IEL/NC) produziram este *Guia de Boas Práticas*.

O propósito é auxiliar gestores e colaboradores das nossas instituições, nacionais e regionais, nos processos de adequação à LGPD e no desenvolvimento de boas práticas de governança.

Dessa forma, pretendemos contribuir com a implementação de programas efetivos de governança no que diz respeito à privacidade de dados pessoais, o que é essencial para a continuidade do nosso bom desempenho na missão de auxiliar o desenvolvimento da indústria brasileira.

Boa leitura.

Robson Braga de Andrade
Presidente da CNI

INTRODUÇÃO

O guia tem como objetivo aprimorar o programa de governança de dados realizado pela Confederação Nacional da Indústria (CNI), pelo Serviço Social da Indústria (SESI), pelo Serviço Nacional de Aprendizagem Industrial (SENAI), pelas federações Estaduais e do Distrito Federal de indústrias e pelo Instituto Euvaldo Lodi (IEL), entidades que, para os fins propostos no presente Guia, conformam o que se convencionam chamar de Sistema Indústria. Além disso, busca apresentar práticas que podem ser adotadas pelas entidades que estão abarcadas pelo âmbito de aplicação deste documento. Para tanto, serão apresentadas as principais operações de tratamento de dados realizados pelas entidades do Sistema Indústria, visando trazer maior segurança e transparência para parceiros, setor público e titulares que se relacionam com essas entidades.

Neste sentido, serão abordadas orientações gerais sobre medidas que podem ser adotadas no processo de implementação de um programa de *compliance* de dados pelas entidades do Sistema Indústria. Dessa forma, serão apresentados exemplos e protocolos gerais e específicos, sendo o guia dividido em três partes.

A primeira parte é voltada para a apresentação dos fundamentos da LGPD, bem como para as especificidades dos procedimentos realizados pelo Sistema Indústria. Serão discutidos o fluxo de dados e as particularidades dos tratamentos realizados, com a necessária análise de sua estrutura da rede nacional, composta pela CNI, além do Departamento Nacional do Serviço Social da Indústria (SESI/DN), do Departamento Nacional do Serviço Nacional de Aprendizagem Industrial (SENAI/DN) e do Núcleo Central do Instituto Euvaldo Lodi (IEL/NC).

A segunda parte do guia traz protocolos gerais aos agentes do Sistema Indústria. Para tanto, são apresentados modelos de protocolos para a garantia dos direitos dos titulares; armazenamento e eliminação de dados; avaliação de risco; segurança da informação e tratamento de dados voltados às atividades de comunicação, por exemplo.

A terceira parte do guia tem como finalidade discorrer sobre recomendações de protocolos específicos do Sistema Indústria. Dessa maneira, será possível abordar as principais hipóteses de tratamento identificadas. Entre os temas abordados estão: educação básica, educação técnica e profissional, e programas socioeducativos voltados às condições de segurança e saúde no ambiente de trabalho.[1]

1 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Sistema indústria**: o motor de desenvolvimento do Brasil. Disponível em: https://www.portaldaindustria.com.br/cni/institucional/sistema-industria/#:~:text=O%20Sistema%20Ind%C3%BAstria%20promove%20e,sa%C3%BAde%20no%20ambiente%20de%20trabalho. Acesso em: 21 jun. 2023.

É certo que para o desempenho das competências do Sistema Indústria, faz-se necessário o tratamento de dados de diversos colaboradores do Sistema Indústria, além de outros *stakeholders* essenciais para realização das iniciativas de toda a rede. Além disso, é importante considerar que a LGPD traz várias possibilidades para o tratamento de dados pessoais e tem como um de seus objetivos contribuir com a inovação e o desenvolvimento econômico, ao estabelecer a segurança jurídica necessária para os agentes de tratamento, ao mesmo tempo em que garante a proteção de dados dos cidadãos.

A lei introduz diversas obrigações aos agentes de tratamento que fazem parte do ecossistema de tratamento de dados, mas também traz diversas possibilidades de atuação para esses atores. Pode-se mencionar, entre elas, a oportunidade de os agentes de tratamento formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento e os procedimentos relacionados ao tratamento de dados pessoais em suas entidades.[2]

Assim, este guia foi elaborado com o objetivo de auxiliar na garantia de proteção dos dados de todos os titulares que se relacionam com o Sistema, ao mesmo tempo em que garante que as atividades das entidades que fazem parte dessa rede sejam desempenhadas, de forma legítima, nas suas diversas frentes de atuação.

Ressalta-se que as orientações aqui trazidas não afastam as recomendações estabelecidas em documentos específicos produzidos por cada uma das entidades e dos órgãos que subscrevem o Guia de Boas Práticas, além de outras boas práticas adotadas pelos órgãos regionais dos Sistemas SESI e SENAI, federações e núcleos regionais do IEL, as quais podem ser aprimoradas e desenvolvidas continuamente.

2 "Art. 50, da LGPD: Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, *poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização*, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais" (grifos nossos).

PARTE 1

PARTE GERAL

1 GLOSSÁRIO

Para auxiliar a leitura e compreensão deste guia, serão apresentados, a seguir, alguns conceitos-chaves sobre proteção de dados e especificidades do Sistema Indústria.

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

Agentes de tratamento: controlador e operador de dados.

Anonimização: procedimentos por meio dos quais um dado perde a capacidade de associação com pessoa física.

Autoridade Nacional de Proteção de Dados (ANPD): responsável pela tutela dos direitos relativos aos dados pessoais dos brasileiros.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

CNI: Confederação Nacional da Indústria, associação sindical de grau superior, que lidera o Sistema Confederativo da Representação Sindical da Indústria, para fins de representação, estudos e coordenação de interesse das categorias econômicas da indústria.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

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

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou 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.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Garantia da segurança da informação: capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

IEL/NC: Núcleo Central do Instituto Euvaldo Lodi, associação sem fins lucrativos, criado sob os auspícios da CNI, do SENAI/DN e SESI/DN, com o objetivo de levar o conhecimento acadêmico às empresas industriais, oferecendo diversos serviços, como agente de integração de estágio, formação executiva e desenvolvimento de carreiras, e como Instituição de Ciência e Tecnologia (ICT), promover a pesquisa e o desenvolvimento em gestão estratégica da Inovação.

Lei Geral de Proteção de Dados (LGPD): Lei nº 13.709, de 14 de agosto de 2018.

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.

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

Operador: pessoa natural ou jurídica, de direito público ou privado que realiza tratamento, conforme instruções do controlador.

Órgão de pesquisa: 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 ou em seu objetivo social ou estatutário, a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, a não ser pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

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.

Relatório de impacto à proteção de dados pessoais (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

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.

SENAI: Serviço Nacional de Aprendizagem. Criado pelo Decreto-Lei nº 4.048/1942, responsável por organizar e administrar, em todo o país, escolas de aprendizagem para industriários, que corporifica órgãos normativos e órgãos de administração, de âmbito nacional e de âmbito regional.

SENAI/DN: Departamento Nacional do SENAI.

SESI: Serviço Social da Indústria, regulamentado por meio do Decreto-Lei nº 57.375/1965, e tem como finalidade auxiliar o trabalhador da indústria e atividades assemelhadas e resolver os seus problemas básicos de existência (saúde, alimentação, habitação, instrução, trabalho, economia, recreação, convivência social, consciência sociopolítica), que corporifica órgãos normativos e órgãos de administração, de âmbito nacional e de âmbito regional.

SESI/DN: Departamento Nacional do SESI.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

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.

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.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

2 CONSIDERAÇÕES INICIAIS

Ao sistematizar as boas práticas no tratamento de dados no Sistema Indústria, este guia busca colaborar com a consolidação da postura proativa do setor no cumprimento dos direitos dos titulares de dados, bem como com o desenvolvimento da cultura de proteção de dados no âmbito do sistema. Além disso, busca-se encorajar a atuação responsável das instituições quanto à transparência e proporcionalidade do tratamento dos dados pessoais, que deve ocorrer de forma adequada e conforme os princípios da proteção de dados estabelecidos na Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD).

Essa estratégia exige, tanto no âmbito nacional como nos âmbitos regionais, a implementação prática de medidas que garantam a efetividade das normas previstas na LGPD. Para concretização dessas e outras recomendações e boas práticas, o documento foi estruturado em três partes e buscou identificar o mapeamento, monitoramento e controle sobre o fluxo de dados existente no Sistema Indústria, apresentando as melhores práticas em matéria de proteção de dados, no Brasil e no exterior.

Nesse contexto, cumpre destacar que a LGPD representou verdadeiro paradigma ao instituir um regime geral de proteção de dados brasileiro. Esse novo paradigma foi reforçado com a inclusão da proteção de dados pessoais no rol de direitos fundamentais da Constituição Federal previstos no art. 5º, LXXIX, após aprovação da Emenda Constitucional nº 115 em fevereiro de 2022. A legislação possui previsões que ampliam a segurança jurídica das atividades de tratamento de dados pessoais, o que favorece o desenvolvimento tecnológico e econômico das diversas entidades e empresas que dependem do tratamento de dados para a realização de suas funções. Isso ocorre por meio de previsões que buscam garantir os direitos dos titulares de dados sem impossibilitar que entes públicos e privados continuem a tratar dados pessoais.

A lei brasileira está inserida no debate mundial de privacidade e proteção de dados, a exemplo da União Europeia, com o Regulamento Geral de Proteção de Dados (RGPD), e Estados Unidos da América, com as leis da Califórnia, *California Consumer Privacy Act* (CCPA), e de Nova Iorque, a *New York Stop Hacks and Improve Electronic Data Security Act* (NY SHIELD).[3]

3 Diferentemente do Brasil e da União Europeia, os Estados Unidos não dispõem de uma regulação federal *ex ante* exclusiva sobre a matéria de proteção de dados, de modo que existem normas a respeito nos estados mencionados, citados para fins de exemplo.

As normas sobre proteção de dados favorecem a criação de um ambiente seguro e propício para o tratamento dos dados pessoais, por meio do qual é garantida a confiança e credibilidade perante o público e demais parceiros empresariais. Isso ocorre devido ao aumento da transparência em relação aos dados que são utilizados, informações sobre como ocorrem os processos de tratamento e desenvolvimento de uma cultura interna capaz de reduzir os riscos de vazamento de informações e prevenir ataques cibernéticos ou outros danos.

Um importante efeito dessas normas pode ser visto no âmbito dos incidentes de segurança. Diversos estudos[4] comprovam que os incidentes relacionados à segurança da informação são minimizados consideravelmente com a adequação de empresas e instituições às leis de proteção de dados.

A relação entre a implementação de práticas de governança, o aumento da *accountability*,[5] a minimização do número de incidentes de segurança e a redução dos atrasos nas vendas foi constatada em estudo publicado pela Cisco, o *Data Privacy Benchmark Study 2020*.[6] Nessa oportunidade, foi observado que mais de 40% das organizações internacionais percebem o dobro de retorno do que foi gasto para implementação de programas de privacidade e proteção de dados pessoais.

Dessa maneira, é evidente que o cumprimento com a legislação voltada à proteção de dados pessoais permite a redução de prejuízos não apenas aos titulares de dados, como às próprias instituições que utilizam os dados em suas atividades. As boas práticas permitem a maior sustentabilidade de inovações por parte de empresas e até mesmo do setor público, uma vez que há incentivos à competitividade, melhoria da credibilidade e confiança com seus pares e o público.

Ademais, também foi constatado o aumento dos retornos financeiros, tanto pela redução dos custos de eventuais violações quanto pelo aprimoramento dos serviços ofertados a partir do adequado tratamento de dados. Sob essa perspectiva, cabe listar, a seguir,

4 Neste sentido, pode-se consultar: IBM Security. **Cost of a Data Breach Report.** 2022. Disponível em: https://www.ibm.com/security/data-breach; EUROPEAN DATA PROTECTION BORD – EDPB. **Guidelines 01/2021 on Examples regarding Data Breach Notification.** Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

5 O termo *accountability* traduz-se em dever fiduciário e, por vezes, em prestação de contas no português. "O dever fiduciário encontra-se no cerne da governança, uma vez que contempla a relação entre o proprietário e o administrador, a quem foi delegado o poder decisório e de gestão de seu patrimônio. A delegação desse poder carrega intrinsecamente a obrigação de sua prestação de contas". Já o conceito de prestação de contas "significa explicar regularmente, qualitativamente e quantitativamente o que foi feito, como e por qual motivo se fez e o que vai ser feito a seguir; bem como justificar aquilo em que se falhou ou deixou de se fazer". ABRAPP. **Código de autorregulação em governança corporativa.** Disponível em: https://www.abrapp.org.br/wp-content/uploads/2021/01/manualautorregulacaocorporativa.pdf.

6 CISCO. 2020 **Data Privacy Benchmark Study**. Disponível em: https://www.cisco.com/c/en_uk/products/security/security-reports/data-privacy-report-2020.html.

alguns dos benefícios obtidos por instituições que implementam programas de governança de dados:[7]

BENEFÍCIOS OBTIDOS POR INSTITUIÇÕES, PÚBLICAS E PRIVADAS, QUE IMPLEMENTAM PROGRAMAS DE GOVERNANÇA DE DADOS (CEDIS/IDP e CIPL)

- Auxilia no cumprimento das exigências legais e regulamentares.
- Proporciona melhor organização dos processos de trabalho das instituições envolvendo dados pessoais.
- Criação de uma cultura de proteção de dados e privacidade nas instituições.
- Auxilia as instituições criar uma relação de fidelização e confiança com clientes, que se sentirão mais seguros com seus dados protegidos.
- Amplia as oportunidades de negócios que envolvem dados pessoais e exigem a adoção de medidas de *compliance* de dados.
- Aumento da confiança com *stakeholders*, por exemplo, mídia, investidores, reguladores, clientes e funcionários.
- Aumento da competitividade e criação de diferencial da instituição que investe em proteção de dados.
- Mitigação de risco sancionatório e redução do impacto financeiro das sanções por conta dos esforços de adequação das instituições.

Além dos benefícios diretamente obtidos pelas instituições que indicam um programa de *compliance* em dados, a iniciativa também contribui com a redução do risco de aplicação das penalidades previstas no art. 52 da LGPD, a exemplo das possibilidades de advertência, aplicação de multa de até 50 milhões de reais por infração ou mesmo a suspensão parcial ou total das atividades que envolvem o tratamento de dados, sem desconsiderar possíveis atuações como as do Procon e Ministério Público.

Você sabia? Boas práticas contribuem com menos custos em casos de incidentes de dados

Segundo estudo publicado pela IBM, **Cost of a Data Breach Report 2021**,[8] que avaliou 537 violações reais de dados em mais de 10 países, é constatado que, no ano de 2021, foi registrado o maior custo médio da violação de dados em 17 anos: passou de USD 3,86 milhões para USD 4,24 milhões.

O mencionado estudo também constatou que as falhas em programas de *compliance*[9] foram o principal motivo que agravou os custos de violação. Conforme analisado, a diferença de custo entre as instituições com alto e baixo nível de falhas de *compliance* chega a 51,1%, com uma diferença em torno de US $2,3 milhões.[10]

Logo, a adoção de um programa de *compliance* de dados permite a todas as entidades do Sistema Indústria manterem e aprimorarem o seu prestígio em um ambiente digital seguro, no âmbito nacional e internacional, além de garantir a proteção dos dados dos atores a elas relacionados. A segurança dos dados dos titulares beneficia diversos atores

7 Informações a partir da pesquisa promovida por CIPL e Cedis/IDP. **Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados** – LGPD. Disponível em: https://www.idp.edu.br/projeto-lgpd.

8 Disponível em: https://www.ibm.com/br-pt/security/data-breach.

9 Trata-se da "adoção de práticas organizacionais voltadas para a criação de processos e de ambiente corporativo que assegure o cumprimento de normas legais". ABRAPP. **Código de autorregulação em governança corporativa**. Disponível em: https://www.abrapp.org.br/wp-content/uploads/2021/01/manualautorregulacaocorporativa.pdf.

10 IBM. **Cost of a Data Breach Report 2021**, p. 27.

públicos e privados, envolvendo os colaboradores do Sistema Indústria, parlamentares, federações, além de beneficiados pelo SENAI, SESI e IEL – que atuam junto à Indústria, uma vez que, acompanhada de um tratamento adequado, medidas de *compliance* de dados contribuem para a eficiência das atividades desenvolvidas em todos os âmbitos e a garantia dos direitos dos cidadãos.

Assim, o **Guia de Boas Práticas para implementação da LGPD no Sistema Indústria** tem como objetivo incentivar o desenvolvimento de processos inovadores, seguros e mais eficientes, que respeitem a autodeterminação informativa e os fundamentos norteadores da proteção de dados, além de contribuir com a efetivação dos propósitos regimentais, regulamentares e estatutários de cada entidade, em prol do empreendedorismo e capacitação da indústria, com desempenho de ações socioeducativas e destinadas à promoção da saúde e segurança no ambiente de trabalho.

3 LEI GERAL DE PROTEÇÃO DE DADOS APLICADA AO SISTEMA INDÚSTRIA

3.1 QUAIS SÃO OS PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS?

Os princípios de proteção de dados estão previstos expressamente no art. 6º da LGPD e fornecem maior segurança e direcionamentos para as organizações que tratam dados pessoais, além de atuarem como forma de garantir maior controle sobre suas informações para o titular.

O ART. 6º DA LGPD APRESENTA OS PRINCÍPIOS DA LGPD:

Boa-fé

O tratamento de dados deve ser pautado nos ditames éticos e morais.

Livre acesso

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidadede seus dados pessoais.

Adequação

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

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.

Prevenção

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

Não discriminação

Impossibilidade de realização do tratamento para fins discriminatórios ou abusivos.

Finalidade

Realização do tratamento para propósitos legítimos, específicos, explícitos, informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Necessidade

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Transparência

Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Segurança

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

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.

3.2 QUAIS SÃO AS BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS?

A LGPD inaugurou uma nova forma de proteção aos dados pessoais, amparada em uma concepção preventiva, também conhecida como o modelo *ex ante* de proteção. Nesse modelo, todo tratamento de dados somente será legítimo caso exista uma previsão legal que justifique aquele tratamento, conforme exposto anteriormente.

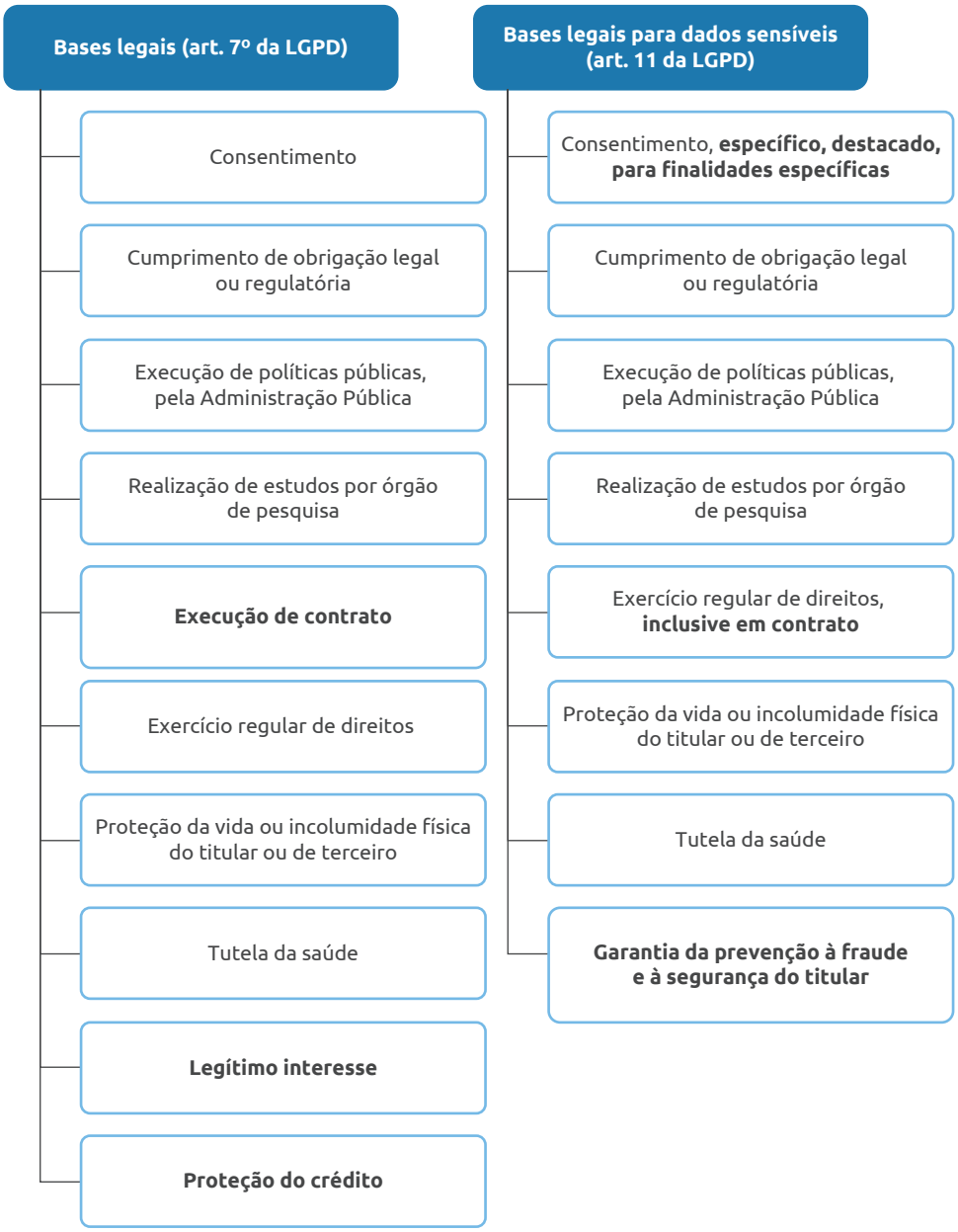
As hipóteses previstas na LGPD que permitem o tratamento de dados pessoais são popularmente conhecidas como "bases legais" e elas relacionam-se diretamente com a finalidade do tratamento. Essa relação garante que o fluxo de dados continue existindo, ao mesmo tempo em que possibilita a proteção daqueles dados tratados. Cada previsão legal traz implicações diferentes, como possibilidade de uso, obrigações e direitos.

Ressalta-se que o regime adotado pela LGPD não faz distinção hierárquica entre as bases legais. Dessa forma, o agente de tratamento deverá verificar a legitimidade de determinado tratamento, a partir da confirmação de existência de base legal adequada para aquele processo.

Além disso, a LGPD trouxe um regime de proteção especial para dados pessoais sensíveis, em razão de seu potencial discriminatório. Os dados sensíveis referem-se às informações "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" (art. 5º, II, LGPD).

Para garantir a efetiva proteção dos dados sensíveis, a LGPD estabelece um número reduzido de bases legais para o seu tratamento. Por isso, ainda no mapeamento dos tratamentos de dados realizados dentro de uma organização, é essencial definir quais dados fazem parte daquele tratamento e se existe base legal adequada para aquele processo, diferenciando o tratamento de dados pessoais do tratamento de dados sensíveis.

Desse modo, durante o mapeamento e o registro das operações de tratamento de dados, o controlador de dados deve indicar qual base legal possibilita cada uma das atividades de tratamento de dados pela entidade, de modo a se assegurar que nenhum tratamento de dados ocorre dentro da instituição sem a devida base legal.



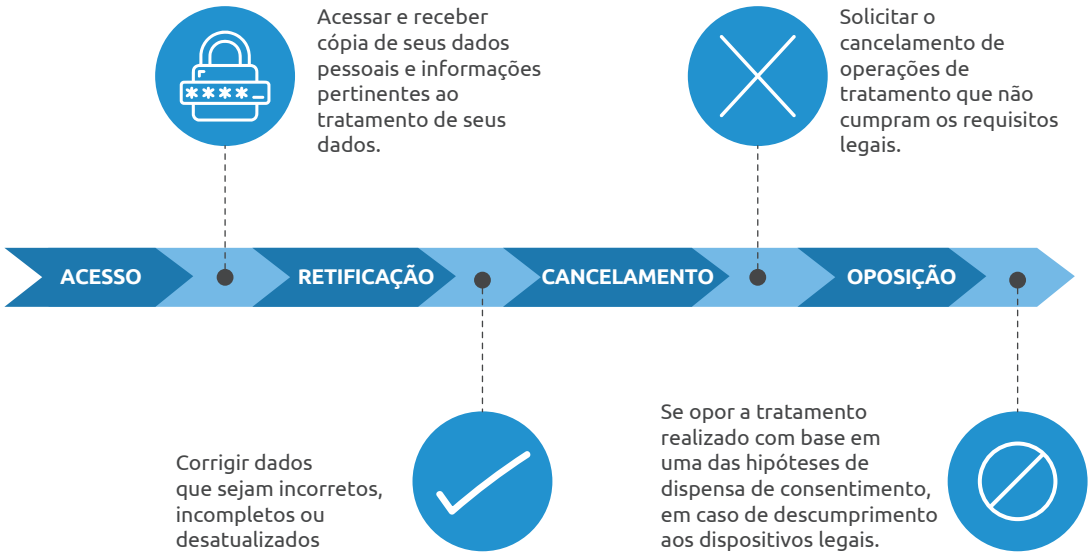
Como grande parte das operações de tratamento de dados do Sistema Indústria envolve o tratamento de dados não sensíveis, as principais bases legais utilizadas pelo Sistema Indústria são o legítimo interesse, a execução de contratos e o cumprimento de obrigação legal ou regulatória. Ainda assim, conforme se verá em detalhes nos protocolos específicos, é necessário um cuidado adicional no tratamento de dados sensíveis, especialmente aqueles que são tratados para a realização de perfis (por exemplo, para seleção de candidatos para bolsas).

3.3 QUAIS SÃO OS DIREITOS DOS TITULARES?

A LGPD enumera diversos direitos que podem ser exercidos pelo titular diretamente à frente do agente de tratamento, pois o sistema brasileiro de proteção de dados pessoais busca garantir e assegurar o controle das informações pessoais pelo titular dos dados.

> Além de reafirmar os **direitos fundamentais** de liberdade de expressão, comunicação e opinião, de intimidade e privacidade, a norma geral enumera outros **direitos operacionais** que têm como objetivo **proteger os dados pessoais dos titulares**.

A partir desse entendimento, o art. 18 da LGPD traz uma série de direitos que buscam garantir o controle do fluxo de seus dados pelo titular. Esses direitos caracterizam os direitos básicos previstos em outras legislações nacionais e internacionais, que são conhecidos pela sigla ARCO, abreviação dos direitos de Acesso, Retificação, Cancelamento e Oposição.[11]



Ademais, a norma ainda prevê outros direitos que garantem maior controle do titular sobre seus dados, além de trazer benefícios econômicos e sociais. Esses direitos estão previstos ao longo do capítulo III da LGPD, que trata especificamente sobre os direitos do titular, os quais estão abrangidos entre os arts. 17, 18, 20 da Lei, conforme imagem a seguir:

11 MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. **Caderno especial Lei Geral de Proteção de Dados.** São Paulo: RT, 2019. p. 35-56.

Direitos do Titular

01. Confirmação da existência de tratamento

02. Correção de dados incompletos, inexatos ou desatualizados

03. Anonimização, bloqueio ou elimiação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD

04. Acesso aos dados

05. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa

06. Eliminação dos dados pessoais tratados com consentimento

07. Receber informações sobre as entidades públicas e privadas com as quais o controlador compartilhou dados pessoais

08. Receber informações sobre a possibilidade de não fornecer o consentimento e as consequências da negativa

09. Revogação do consentimento

10. Direito de petição perante a ANPD ou órgãos de defesa do consumidor

11. Direito de oposição em caso de descumprimento à LGPD

12. Direito de revisão de decisões automatizadas

3.4 QUEM SÃO OS AGENTES DE TRATAMENTO DE DADOS?

De acordo com as definições da LGPD, os agentes de tratamento são o controlador e o operador de dados pessoais. O primeiro é o responsável pelas decisões referentes ao tratamento de dados pessoais. Já o segundo é aquele que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, inciso X, da LGPD), ou seja, é quem realizará o tratamento conforme as instruções fornecidas pelo controlador, verificando a observância das próprias instruções e normas sobre o tema (art. 39 da LGPD).[12]

12 ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado** (2021). Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

Você sabia que?

O **controlador** é o responsável pelas decisões referentes ao tratamento de dados pessoais.

- O controlador definirá, por exemplo, todas as decisões sobre o processamento dos dados pessoais, como a finalidade para quais os dados pessoais serão usados, sob qual justificativa legal (base legal), sobre quais indivíduos os dados serão coletados e quanto tempo eles serão tratados pela instituição.

Ao **operador** compete a realização de tratamentos de dados pessoais em nome do controlador.

- O operador seguirá as instruções fornecidas pelo controlador e, assim, deve realizar o tratamento dos dados pessoais.

A definição do papel ocupado pelos agentes de tratamento envolvidos é feita a partir da **avaliação contextual e fática de cada operação de tratamento de dados**. Assim, uma instituição pode ser controladora e operadora de dados, a depender da atividade analisada.

O controlador de dados pessoais é responsável pelas decisões referentes aos elementos essenciais para o cumprimento da finalidade do tratamento. Logo, o controlador será sempre responsável pela definição:[13]

i) da finalidade do tratamento, com respectivos objetivos que justificam o tratamento de dados realizado, definindo a base legal correspondente;

ii) dos meios de tratamento dos dados pessoais;

iii) dos tipos de dados pessoais tratados, incluindo a natureza dos dados pessoais que fazem parte do tratamento;

iv) da duração do tratamento, com previsão do período de duração da operação de tratamento e definição do prazo para eliminação dos dados.

Esse agente de tratamento pode, ainda, definir outros critérios do tratamento, assim como outros fatores podem ser considerados essenciais ao processamento de dados pessoais, desde que seja considerado o contexto do tratamento.

As definições dos elementos essenciais do tratamento servem como instruções para o operador de dados pessoais, uma vez que esse agente de tratamento só pode agir conforme as determinações do controlador, sob pena de o operador ser equiparado ao controlador de dados. Ou seja, o operador deve seguir as instruções do controlador. Normalmente, os operadores de dados pessoais são contratados pelos controladores de dados para desempenhar certas atividades de tratamento, como, por exemplo, quando uma instituição contrata empresa de *call center* para entrar em contato com o público inscrito em eventos.

13 ANPD. **Guia orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Versão 2.0. Abril de 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf.

Por isso, é imprescindível que tais contratos estabeleçam o regime de atividades e responsabilidades entre o operador e o controlador. Contudo, considerando as relações existentes entre as organizações que compõem o Sistema Indústria, é possível que tal regime seja estabelecido por meio de outros instrumentos jurídicos, como portarias, leis, códigos e condutas, diretrizes e normas internas.

Além disso, considerando que o operador pode subcontratar outras pessoas jurídicas ou naturais para participar do tratamento de dados, é obrigação de o operador informar o controlador sobre qualquer contratação de suboperador. Exemplos comuns de subcontratação podem identificados na contratação de serviços de armazenamento de dados pessoais em nuvem para auxiliar na execução da atividade para a qual o operador foi contratado.

Os agentes de tratamento podem ser pessoas naturais ou jurídicas, de direito público ou privado. O Sistema Indústria é composto por diversas pessoas jurídicas privadas, com autonomia, de forma que essas pessoas, a depender do tratamento, atuarão como controlador ou operador de dados pessoais.

Vale indicar que, embora não seja o responsável pelas decisões sobre os elementos essenciais, o operador pode decidir sobre o sistema, método e/ou ferramentas a serem utilizadas para a coleta de dados pessoais; a forma de armazenamento, se no meio físico ou digital; os meios pelos quais os dados podem ser transferidos de um setor para o outro; as modalidades de assegurar a retenção dos dados.[14]

Conforme orientações da ANPD, controlador e operador compartilham obrigações a respeito do tratamento de dados, tais como a necessidade de garantir as condições legais para que o tratamento ocorra, de forma que ambos possuem a responsabilidade de manter o registro das operações de tratamento.

Não obstante, as responsabilidades dos atores "são determinadas de acordo com o papel exercido por cada um no âmbito do tratamento dos dados pessoais,"[15] mesmo que o controlador tenha a principal responsabilidade e o operador atue em nome dele.

14 KREMER, Bianca. Os agentes de tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020, 9. 306.

15 ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Versão 2.0. Abr. 2022, p. 18. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf.

3.5 QUEM É O ENCARREGADO PELO TRATAMENTO DE DADOS?

O encarregado dos dados, ou *Data Protection Officer* (DPO), é figura central no sistema de proteção de dados, sendo "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados."[16]

Dessa forma, o encarregado deve atuar como principal ponto de contato entre a organização e os titulares de dados e, ainda, entre a organização e a ANPD. O encarregado ainda deve assessorar e orientar a organização sobre proteção de dados e conformidade com a LGPD.[17]

Com tais objetivos, o encarregado pode desempenhar algumas funções que se relacionam com esse papel central de diálogo entre os agentes do ecossistema de tratamento de dados pessoais:[18]

i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências (art. 41, §2º, I, da LGPD);
ii) receber comunicações da ANPD e adotar providências (art. 41, §2º, II, da LGPD);
iii) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (art. 41, §2º, III, da LGPD);
iv) manter e atualizar o registro das operações de tratamento de dados pessoais (art. 37 da LGPD);
v) participar das avaliações de risco aos direitos e liberdades fundamentais do titular (art. 38 da LGPD);
vi) identificar as bases legais aplicáveis ao tratamento de dados (arts. 7º e 11, art. 41, §2º, da LGPD);
vii) responder os titulares sobre questionamentos sobre os tratamentos de dados (art. 5º, VIII, e art. 41, §2º, da LGPD);
viii) participar na notificação e na gestão de incidentes de segurança envolvendo dados pessoais (art. 46 da LGPD);
ix) realizar ou participar de auditorias – internas ou de parceiros;[19]
x) elaborar políticas, processos, controles e outros modelos internos relevantes;[20]

16 Apesar da definição constante no art. 5º, VIII, da LGPD mencionar que o encarregado é pessoa indicada pelo controlador e operador, a legislação indica que a indicação é obrigatória apenas nas atribuições do controlador (art. 41 da LGPD).

17 CIPL; CEDIS. **O papel do/a Encarregado/a conforme a Lei Geral de Proteção de Dados Pessoais.** 2021. Disponível em: https://www.idp.edu.br//arquivos/cedis/artigo-encarregado-lgpd-efetiva.pt.pdf. Acesso em: 21 jun. 2023.

18 *Idem, ibidem.*

19 *Idem, ibidem.*

20 *Idem, ibidem.*

xi) participar da negociação de contratos que envolvam dados pessoais;[21] e
xii) oferecer treinamento e planejar atividades de conscientização.[22]

É importante ressaltar que o cargo de encarregado pode ser exercido tanto por pessoa física quanto por pessoa jurídica e pode ser um membro ou time da organização ou, ainda, um agente externo.

O encarregado é essencial para garantir a comunicação entre a organização a qual ele(a) representa, os titulares de dados e a ANPD. Dessa forma, é essencial que ele tenha amplo conhecimento e familiaridade sobre as atividades de tratamento desempenhadas pela entidade representada.

Tendo em vista a complexa composição do Sistema Indústria e as diferentes atividades desempenhadas por cada uma das entidades que o compõem, são diversas as possibilidades de indicação do encarregado. A decisão sobre as atribuições do encarregado deve levar em consideração a otimização de suas funções, a capacidade de desempenho de suas atividades e sua independência. Por exemplo, no âmbito das entidades e órgãos nacionais do Sistema Indústria (CNI, SESI/DN, SENAI/DN e IEL/NC), foi indicado um único encarregado para as quatro.

As diferentes configurações, contudo, não afastam a obrigação de cada uma das entidades e órgãos publicar informações para contato com o encarregado, que deve ser feita por meio dos sítios eletrônicos de cada um. Nessa oportunidade será disponibilizado meio para contato com o encarregado, de preferência, via *e-mail*. Esse processo pode ser automatizado por formulário eletrônico que encaminha as requisições diretamente para o canal de atendimento do encarregado.

As informações para contato especificamente com o encarregado sobre a matéria de proteção de dados pessoais poderão estar disponíveis nas abas do Serviço de Atendimento ao Cidadão (SAC), em cada um dos *sites* das entidades e órgãos que compõem o Sistema Indústria.

3.6 QUAL O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS NA APLICAÇÃO DA LGPD?

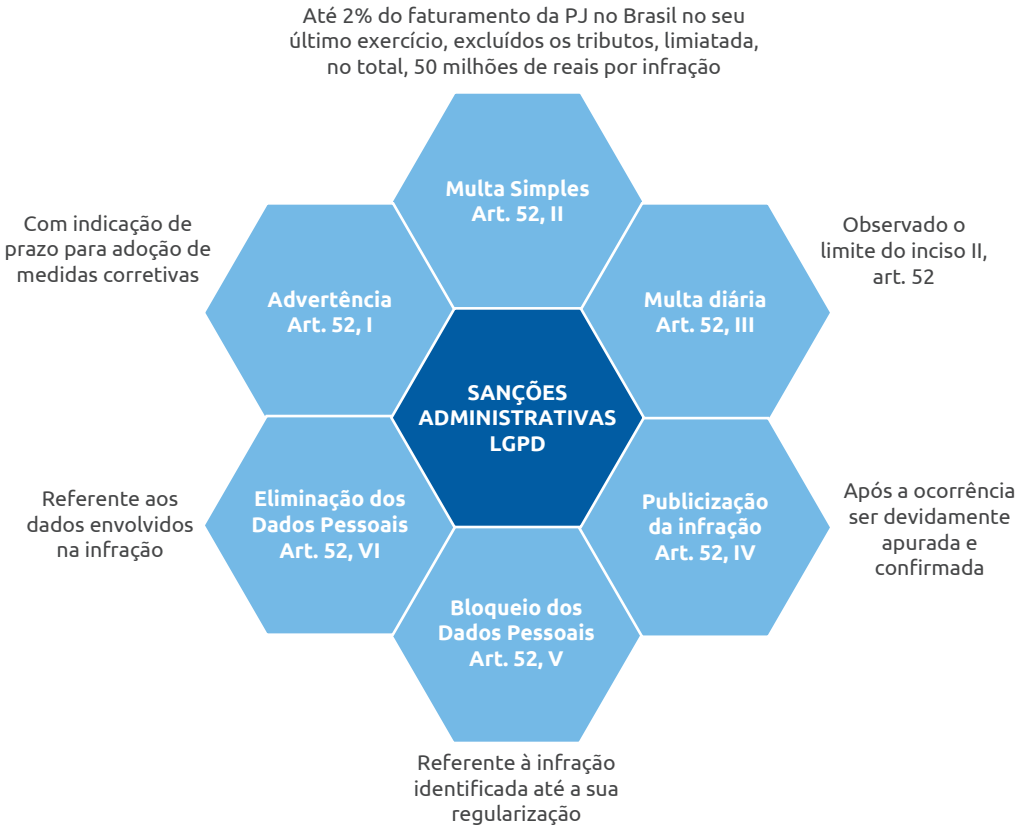
A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão público responsável por zelar pela aplicação da LGPD. Desse modo, a ANPD possui papel fiscalizador das disposições

21 *Idem, ibidem.*
22 *Idem, ibidem.*

da lei e é o agente competente para determinar ações no âmbito da proteção de dados, incluindo aplicação de sanções.

Desde 1º agosto de 2021, as sanções administrativas previstas nos arts. 52 a 54 da LGPD estão em vigor no Brasil.[23] Na LGPD, é previsto um rol diverso de sanções, de natureza admoestativa (advertência e publicização), pecuniária (com pagamento de multas na moeda brasileira) e restritiva de atividades (ou seja, os agentes ficam proibidos de exercer a atividade punida com dados pessoais). Dessa forma, é possível observar o incentivo à cooperação e responsabilidade dos agentes de tratamento de dados em adotar medidas que evidenciem o cumprimento das normas de proteção de dados.[24]

Confira, a seguir, as seis possibilidades de sanções administrativas dispostas no art. 52 da LGPD:



23 A respeito, vale considerar que a ANPD vem trabalhando na regulamentação destes dispositivos, por meio da viabilização de consultas públicas sobre o Regulamento de Dosimetria e Aplicação de Sanções Administrativas que envolvem, por exemplo, a metodologia que orienta o cálculo do valor-base das sanções de multas a serem aplicadas por descumprimento à Lei Geral de Proteção de Dados. BRASIL. Autoridade Nacional de Proteção de Dados. **Regulamento de dosimetria e aplicação de sanções administrativas**. 2022. Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-dosimetria-e-aplicacao-de-sancoes-administrativas. Acesso em: 21 jun. 2023.

24 WIMMER, Miriam. Os desafios do *enforcement* na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. *In*: MENDES, Laura Schertel *et al.* (Coords.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021.

Além disso, o art. 52, em seu §1º, dispõe que as sanções serão analisadas de forma isolada ou cumulativa, conforme as peculiaridades de cada caso concreto e em consideração ao seguinte:

i) a gravidade e a natureza das infrações e dos direitos pessoais afetados;
ii) a boa-fé do infrator;
iii) a vantagem auferida ou pretendida pelo infrator;
iv) a condição econômica do infrator;
v) a reincidência;
vi) o grau do dano;
vii) a cooperação do infrator;
viii) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 da LGPD;
ix) a adoção de política de boas práticas e governança;
x) a pronta adoção de medidas corretivas; e
xi) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Especificamente quanto às multas diárias, o art. 54 da LGPD estabelece que o valor da sanção deve "observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela Autoridade Nacional", e é requisito que a sua intimação contenha, "no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento."[25]

Há incentivos aos agentes que realizam o tratamento de dados pessoais a desenvolverem estratégias que minimizem os riscos de incidência das infrações dispostas na Lei, bem como a evitar que as condutas erradas não se repitam. A rapidez de resposta em caso de violações à proteção de dados também se mostra importante fator na aplicação de sanções e, para isso, políticas de boas práticas e governanças por cada entidade e órgão são apontadas como relevantes.

25 "Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional. Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento."

Nesse sentido, de acordo com a própria ANPD, as opções de sanções estão fundadas em um plano de monitoramento do setor que possibilite a priorização de temas de acordo com o seu risco, gravidade, atualidade e relevância.[26]

A respeito das sanções administrativas, o art. 53 da LGPD estabelece que a Autoridade definirá as metodologias que orientarão o cálculo do valor-base das sanções de multa por meio de regulamento próprio, as quais também devem ser objeto de consulta pública.[27]

A Resolução CD/ANPD nº 1, de 28 de outubro de 2021,[28] regulamenta o processo de fiscalização e administrativo sancionador no âmbito da ANPD. Neste documento é estabelecido que a autoridade adotará atividades de monitoramento, orientação e prevenção no processo de fiscalização para poder iniciar a atividade repressiva (art. 15) e, de acordo com o art. 70, o primeiro ciclo de monitoramento teve início a partir de janeiro de 2022.

Nesse sentido vale mencionar a Resolução nº 01/2021 da ANPD, que apresenta o seu Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador. Este documento alcança a fiscalização das atividades de monitoramento dos titulares de dados, agentes de tratamento, pessoas naturais ou jurídicas, de direito público ou privado e demais interessados no tratamento de dados pessoais, e conta com aplicação subsidiária da Lei nº 9.784/99, a qual regula o processo administrativo no âmbito da Administração Pública Federal.[29]

Ademais, em 2023, a ANPD publicou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas[30], por meio da Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. No documento, foram estabelecidos os critérios e parâmetros para aplicação das sanções pecuniárias e não pecuniárias, além das formas e o método de cálculo para o valor-base das sanções de multa.

---

26 BRASIL. Autoridade Nacional de Proteção de Dados. **Sanções administrativas:** o que muda após 1º de agosto de 2021. out. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021. Acesso em: 21 jun. 2023.

27 "Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa."

28 BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 1, de 28 de outubro de 2021**. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acesso em: 21 jun. 2023.

29 Art. 1º, §§1º e 2 do BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 1, de 28 de outubro de 2021**. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acesso em: 21 jun. 2023.

30 ANPD. **Regulamento de Dosimetria e Aplicação de Sanções Administrativas**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria.

Conforme apresentado pela Autoridade, as infrações possuem três níveis:

Três níveis de classificação de gravidade da infração à LGPD

Leve	Média	Grave
Quando a infração não for média ou grave.	Infrações que (i) afetem significativamente interesses e direitos fundamentais dos titulares; (ii) desde que não sejam classificadas como graves.	I. Infrações Médias: (i) tratamento em larga escala; OU (ii) auferir ou pretender auferir vantagem econômica; OU (iii) risco à vida ou à integridade física dos titulares; OU (iv) uso de dados sensíveis, de crianças, adolescentes ou idosos; OU (v) ausência de base legal; (vi) tratamento com efeitos discriminatórios ilícitos ou abusivos; (vii) verificada a adoção sistemática de práticas irregulares. II. Obstrução à atividade de fiscalização.

Vale considerar que, além de cumprir com sua função fiscalizadora e sancionadora, a ANPD também busca desenvolver a conscientização dos direitos e deveres previstos na lei, incentivando a colaboração com demais agentes, inclusive, o próprio Sistema Indústria.

Observa-se, então, que foram previstos incentivos aos agentes que realizam o tratamento de dados pessoais a desenvolverem estratégias que minimizem os riscos de incidência das infrações dispostas na Lei, bem como a evitar que as condutas erradas não se repitam. A rapidez de resposta em caso de violações à proteção de dados também se mostra importante fator na aplicação de sanções e, para isso, políticas de boas práticas e de governanças pelas entidades e órgãos, são indicados como relevantes.

4 MARCO NORMATIVO

O sistema de proteção de dados é marcado por diversas normas regulatórias que devem ser aplicadas conjuntamente, a exemplo da Constituição Federal de 1988, Código Civil (Lei nº 10.406/2002) e Marco Civil da Internet (Lei nº 12.965/2014). O Sistema Indústria conta, ainda, com diversas leis e normas específicas sobre o âmbito de atuação de suas entidades e órgãos. Dessa forma, as seguintes normas, em ordem cronológica e trazidas em lista exemplificativa, devem ser aplicadas conjuntamente às regras de proteção de dados, a fim de observância de todas as previsões legais.

- **Decreto-Lei nº 4.048/1942** – cria o Serviço Nacional de Aprendizagem dos Industriários (SENAI).
- **Lei nº 5.452/1943 (CLT)** – consolida a Legislação Trabalhista, estabelece regras sobre o sistema de aprendizagem, que no âmbito da indústria, deve ser atendido prioritariamente pelos serviços nacionais de aprendizagem, entre eles, o SENAI.
- **Decreto-Lei nº 9.403/1946** – autoriza a CNI a criar e organizar o SESI, e institui, em seu favor, a contribuição compulsória devida pelas empresas, indústrias, de transportes, de comunicações e de pesca.
- **Decreto nº 494/1962** – aprova o Regimento do Serviço Nacional de Aprendizagem Industrial.
- **Decreto n° 57.375/1965** – aprova o Regulamento do SESI, cuja elaboração é de iniciativa da CNI.
- **Lei nº 8.443/1992** – dispõe sobre a organização do TCU e estabelece que sua jurisdição abrange as entidades privadas que recebam contribuições fiscais.
- **Lei nº 11.457/2007** – dispõe sobre a Receita Federal do Brasil e sobre a arrecadação, mediante remuneração, das contribuições incidentes sobre a folha salarial devidas a terceiros (a exemplo dos Serviços Sociais Autônomos).
- **Lei nº 11.788/2008** – dispõe sobre o estágio de estudantes e outras providências.
- **Lei nº 12.513/2011** – confere autonomia aos serviços sociais nacionais para criar unidades de ensino para a oferta de educação profissional técnica de nível médio e educação de jovens e adultos integrada à educação profissional.
- **Resolução nº 25/2016** – estabelece, no âmbito do SENAI, diretrizes sobre medidas de aumento da transparência, em especial por meio da utilização dos sítios das entidades na rede mundial de computadores (internet).

- **Resolução nº 75/2016** – estabelece, no âmbito do SESI, diretrizes sobre medidas de aumento da transparência, em especial por meio da utilização dos sítios das entidades na rede mundial de computadores (internet).
- **Lei nº 14.436/2022** – dispõe sobre as diretrizes para a elaboração e a execução da Lei Orçamentária de 2023 e dá outras providências.[31]
- **Lei nº 14.600/2023** – estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios; altera as Leis nºs 9.984, de 17 de julho de 2000, 9.433, de 8 de janeiro de 1997, 8.001, de 13 de março de 1990, 14.204, de 16 de setembro de 2021, 11.445, de 5 de janeiro de 2007, 13.334, de 13 de setembro de 2016, 12.897, de 18 de dezembro de 2013, 8.745, de 9 de dezembro de 1993, 9.069, de 29 de junho de 1995, e 10.668, de 14 de maio de 2003; e revoga dispositivos das Leis nºs 13.844, de 18 de junho de 2019, 13.901, de 11 de novembro de 2019, 14.261, de 16 de dezembro de 2021, e as Leis nºs 8.028, de 12 de abril de 1990, e 14.074, de 14 de outubro de 2020.
- **Resolução nº 018/2019** – determina, no âmbito do SENAI, a adoção de programas de *compliance*.
- **Resolução nº 049/2019** – determina, no âmbito do SESI, a adoção de programas de *compliance*.
- **Instrução de Serviço Conjunta nº 01/2020** – institui a Política de Segurança da Informação no âmbito da CNI, do SESI/DN, do SENAI/DN e do IEL/NC.

31 A Lei de Diretrizes Orçamentárias (LDO) estabelece as regras para a elaboração da Lei Orçamentária Anual do ano seguinte, portanto, a legislação de referência é atualizada periodicamente.

5 SISTEMA INDÚSTRIA: FLUXO DE DADOS E ESPECIFICIDADES

5.1 FINALIDADES DO TRATAMENTO DE DADOS REALIZADO PELO SISTEMA INDÚSTRIA

Para os fins propostos no presente Guia, o Sistema Indústria é uma rede nacional de caráter privado formado pela Confederação Nacional da Indústria (CNI), pelas federações dos Estados e do Distrito Federal e que lhe forem filiadas.[32]

Também compõem o Sistema Indústria: (i) o Sistema Serviço Social da Indústria (SESI), por meio de seus órgãos nacionais e regionais; (ii) o Sistema Serviço Nacional de Aprendizagem Industrial (SENAI), por meio de seus órgãos nacionais e regionais; e (iii) o Sistema Instituto Euvaldo Lodi (IEL), também com entidades nacional e regionais.[33]

A CNI possui o propósito de representar e coordenar ações e estudos de interesses das categorias econômicas do setor industrial. Assim, atua "na defesa e na promoção de políticas públicas que favoreçam o empreendedorismo e a produção industrial, num setor que reúne mais de 476 mil indústrias no país."[34]

Em acréscimo, as federações de indústrias estão presentes nos 26 estados e Distrito Federal, atuando na defesa e representação das indústrias locais perante os governos estaduais e municipais. Por meio delas, há a conexão desses atores locais com a CNI, que ocorre por fornecimento de informações gerais sobre o panorama geral da indústria, bem como auxiliando no desenvolvimento de projetos específicos.

32 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Sistema indústria**: o motor de desenvolvimento do Brasil. Disponível em: https://www.portaldaindustria.com.br/cni/institucional/sistema-industria/#:~:text=O%20Sistema%20Ind%C3%BAstria%20promove%20e,sa%C3%BAde%20no%20ambiente%20de%20trabalho. Acesso em: 21 jun. 2023.

33 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Estatuto**. Art. 9º. 2021. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/a9/51/a9512d68-a152-40dd-866d-8cd68d8c9f2d/estatuto_da_cni.pdf. Acesso em: 21 jun. 2023.

34 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Áreas de atuação**. 2023. Disponível em: https://www.portaldaindustria.com.br/cni/institucional/. Acesso em: 21 jun. 2023.

Dessa maneira, o Sistema Indústria é composto por diversas entidades que contam com variados graus e natureza de autonomia de suas atividades. Assim, não apenas os tipos de dados pessoais tratados, como as finalidades e exigência de compartilhamento das informações nos âmbitos regionais e nacional possuem características específicas.

Ademais, depreende-se que as entidades que atuam nele desenvolvem serviços com objetivos complementares, mas voltados a diferentes fins específicos. Exemplos nesse sentido são a promoção de eventos institucionais que buscam aproximar a Indústria de demais setores econômicos, bem como atividades que promovem a segurança do trabalhador ou intermediação de estágio, de modo a integrar o Sistema Indústria por meio da promoção da qualificação das pessoas e qualidade no ambiente de trabalho.

Todas essas atividades que envolvem o tratamento de dados pessoais devem ocorrer conforme os limites legais da LGPD, ou seja, conforme as bases legais previstas pela própria Lei.

Por ora, é válido destacar a intrínseca relação entre as bases legais e os princípios da LGPD, vez que ambos integram as condições de legitimidade para o tratamento de dados. Isto é, para que um tratamento de dados seja considerado lícito, é preciso haver tanto uma base legal autorizativa, como também a compatibilidade com os princípios previstos no art. 6º da LGPD.

Entre os princípios previstos no artigo, destacam-se o princípio da finalidade, previsto no inciso I do art. 6º da LGPD. Dessa maneira, busca-se evitar que os dados sejam coletados, armazenados e tratados de forma irrestrita, para além dos objetivos que seriam necessários e com outras finalidades não previstas originalmente.

Assim, é importante discorrer acerca das principais finalidades pelas quais ocorre o tratamento de dados no Sistema Indústria, comumente associadas aos objetivos institucionais das entidades – promoção do desenvolvimento industrial, educação, cultura, saúde e segurança dos trabalhadores, aumento da competitividade e desenvolvimento sustentável.

5.1.1 SISTEMA INDÚSTRIA

As operações de tratamento de dados pessoais realizadas pelo Sistema Indústria são complexas e envolvem um conjunto variado de dados pessoais, a exemplo do público externo, a quem são destinados a maioria de seus serviços e produtos; como também de seus colaboradores, o que envolve tanto dados pessoais quanto dados sensíveis, conforme a finalidade pretendida.

No âmbito interno de todas as entidades, é possível indicar o uso de dados quanto à contratação de seus colaboradores, envolvendo as fases (i) pré-contratual, como currículos e cartas de motivação; (ii) contratual, como exames admissionais e informações pertinentes à contratação; (iii) execução contratual, como registro de jornada e administração da folha de pagamento; e (iv) pós-contratual, com armazenamento e exclusão dos dados conforme prazo prescricional.

Os dados das áreas responsáveis pelo gerenciamento dos Recursos Humanos envolvem cópia de documentos pessoais, carteira de trabalho, informações sobre cônjuge e filhos, dados bancários, folha de ponto, entre outros, que podem ocorrer sob o crivo das bases legais do cumprimento de obrigação legal ou regulatória; execução ou criação de contrato e exercício regular de direitos, de forma exemplificativa.

Os dados coletados a partir dos próprios colaboradores também são importantes para o regular funcionamento das atividades do Sistema Indústria. Informações, como nome e *e-mail*, são utilizadas para armazenamento, cadastro e criação de perfis em sistemas internos, para que sejam desempenhadas suas funções. Restrições de acesso a dados em sistemas também podem ser geradas a partir disso, pois cargos de liderança e gestão podem ter maior autonomia em acessar a completude dos dados, em relação a cargos que não exigem este acesso.

Como se verá adiante, esta restrição de acesso é importante medida para assegurar que os dados armazenados não sejam indevidamente acessados e que as informações tratadas atinjam sua finalidade.

Quanto às atividades de pesquisa, gestão do relacionamento com clientes e captação e operação de contratos de base nacional, pretende-se, em suma, utilizar os dados fornecidos pelos titulares – empresas e/ou instituições, representantes legais; podendo incluir dados sensíveis em especial no último item – para elaboração de pesquisas, prospecção e abordagem de clientes, e estabelecimento de contratos.

Aqui, há grande relevância do sistema CRM,[35] por meio do qual os dados são agregados, permitindo a identificação e contato com pessoas físicas e jurídicas que não pertencem ao Sistema Indústria. No caso das três atividades citadas no parágrafo anterior, o CRM é utilizado para manutenção e atualização da base de contatos consecutivos.

Este sistema também é utilizado pela CNI para diversas modalidades de comunicação externa, como o *mailing* de imprensa, abrangendo dados de contato e identificação de profissionais do ramo, como jornalistas e editores.

35 *Customer Relationship Management*: Sistema de Gestão de Relacionamento com o Cliente.

Em todos os seus níveis o funcionamento do Sistema Indústria demanda a comunicação interna e externa entre colaboradores e com outros membros e parceiros relacionados ao sistema e recorrentemente são utilizadas ferramentas como o *e-mail*, *WhatsApp* e a plataforma *Microsoft Teams*.

Dada a importância desses meios de comunicação, na Parte II deste guia abordaremos o uso de aparelhos privados, institucionais ou não, e sistemas de mensageria privada, os quais, embora não sejam adotados oficialmente, são comumente utilizados pelos colaboradores, isto é, empregadores e gestores em todos os níveis.

Além disso, as informações de natureza financeira, patrimonial e econômica, bem como contratuais são objeto de auditorias externas independentes e por órgãos de controle, como é o caso do Tribunal de Contas da União (TCU), que exerce controle finalístico sobre as contas do SESI e do SENAI.

Ressalta-se que a flexibilidade e a cooperação entre os agentes envolvidos favorecem uma atuação em rede, por meio de órgãos, nos casos do SENAI e SESI, e núcleos; no caso do IEL, regionais e nacional, distribuídos pelo Brasil. Por isso, é possível – e incentivado – que as atividades econômicas se desenvolvam a partir de boas práticas no âmbito de proteção de dados, as quais conferem maior segurança para o titular, e contribuem com a constante inovação e aperfeiçoamento dos serviços prestados.

Além das atividades comuns a todos os membros do Sistema Indústria, também existem operações de tratamento de dados que são específicas de cada uma das entidades ou órgãos. Assim, serão apresentadas tais particularidades nos itens que se seguem.

5.1.2 CNI

A CNI atua no intermédio de comunicação entre os setores industriais e agentes privados com agentes públicos, atuando na representação, defesa e coordenação dos interesses gerais da indústria. O desenvolvimento de relações com autoridades que permitam a defesa dos interesses desse setor econômico é uma das principais finalidades que justificam o tratamento de dados, que serão objeto de maiores considerações na Parte III do presente guia.

Dada essa função, a CNI por vezes representa o setor em processos administrativos ou judiciais, no exercício de direitos, prioritariamente no Supremo Tribunal Federal (STF), Superior Tribunal de Justiça (STJ) e Tribunal Superior do Trabalho (TST). Note-se que a CNI é legitimada para propor ações de controle concentrado perante o STF, atuar como *amicus curiae* ou apenas acompanhar o progresso de processos judiciais sem intervir diretamente nos autos. Assim, a CNI apresenta os processos a partir de três perspectivas

de sua atuação: (i) ações em que é autora; (ii) ações em que é *amicus curiae*; (iii) ações em que é observadora, elaborando, inclusive, a Agenda Jurídica da Indústria.

Ademais, a CNI também elabora a Agenda Legislativa da Indústria,[36] em conjunto com as federações de indústrias e associações setoriais de âmbito nacional, que dispõe sobre as proposições com potencial de impacto e relevância para o setor industrial. Este é um dos produtos viabilizados pelo compartilhamento de informações e comunicação exercida internamente no Sistema Indústria, voltado à defesa de interesses do setor perante o Poder Legislativo, com objetivo de colaborar com melhorias no ambiente de negócios, alcançando o setor industrial e a sociedade.

5.1.3 SENAI E SESI

Como mencionado previamente, o SENAI e o SESI são conformados em órgãos normativos e executivos, nacionais e regionais. Os Departamentos Nacionais são órgãos administrativos de âmbito nacional, responsáveis por promover, executivamente, os objetivos institucionais, nos setores técnico, operacional, econômico, financeiro, orçamentário e contábil, segundo os planos e as diretrizes adotados pelos Conselhos Nacionais de cada Entidade, em âmbito local.

A respeito do SENAI, grande parte dos dados tratados envolvem informações de alunos, bolsistas, pesquisadores e trabalhadores, em especial por meio da oferta de cursos em todos os níveis da educação profissional e tecnológica.

Ademais, vale destacar a existência dos Institutos SENAI de Inovação (ISI) e os Institutos SENAI de Tecnologia, especializados em prestação de consultorias técnicas e desenvolvimento de produtos e processos inovadores. Logo, os dados tratados possuem o propósito de possibilitar a execução dos serviços contratados, voltados à priorização de contato entre a indústria e a academia, assim como a aplicação de boas práticas internacionais aos mais diversos perfis industriais.

Os Institutos SENAI de Tecnologia destinam-se ao apoio de pequenas, médias e grandes empresas para que se mantenham atualizadas tecnologicamente para aumentar sua competitividade nos planos nacional e internacional, lidando com os dados relativos aos contratos estabelecidos com diferentes representantes das áreas econômicas como Automotiva e Tecnologia da Informação, por exemplo.[37]

---

36 A edição de 2022 e dos anos anteriores da **Agenda Legislativa da Indústria** pode ser consultada publicamente *on-line* em: https://www.portaldaindustria.com.br/cni/canais/assuntos-legislativos/produtos/agenda-legislativa/#agenda-legislativa-da-industria-2022%20.

37 SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI. **Relatório anual**: SESI-SENAI-IEL 2018. Brasília: SESI/DN, 2019. p. 24; SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL (SENAI). **Institutos SENAI de Inovação**. Disponível em: https://www.portaldaindustria.com.br/senai/canais/instituto-senai-de-inovacao/. Acesso em: 21 jun. 2023.

O SESI desenvolve atividades voltadas à indústria e aos trabalhadores, seus dependentes e comunidade.[38] Para isso, promove ações destinadas à qualidade de vida, educação, segurança e medicina do trabalho, mercado de trabalho, assistência social, saúde, cultura, esporte e lazer, questões de sustentabilidade, responsabilidade social e competições relacionadas à educação.

Por meio de seu Departamento Nacional, o SESI atua na "definição das diretrizes estratégicas e na formulação de soluções para o negócio, inclusive por meio da alocação de recursos financeiros em programas e projetos de interesse nacional e regionais."[39]

O SESI conta com departamentos regionais que tratam dados de alunos, bolsistas, pesquisadores e trabalhadores. Sua função é promover a colaboração e articulação com estabelecimentos contribuintes, visando à uniformidade do sistema nacional de serviço social e respeito às peculiaridades das regiões brasileiras (art. 13 do Regulamento do Serviço Social da Indústria).

Um dos serviços que requer o tratamento de dados e possui grande destaque é a plataforma digital *SESI Viva+*. Essa plataforma reúne dados sobre Segurança e Saúde no Trabalho (SST) e estilo de vida do trabalhador da indústria, permitindo análises e estudos epidemiológicos por meio do fornecimento de informações estruturadas sobre saúde, consumo e preferências dos trabalhadores à indústria.[40]

De acordo com o Mapa da Saúde dos Trabalhadores da Indústria atendidos pelo SESI Viva+[41], o SESI atendeu, em 2021, empresas no país que somam mais de 900 mil trabalhadores ativos, dos quais sete em cada dez são homens, grupo composto majoritariamente por jovens entre 25 e 39 anos,[42] por exemplo. Dados sobre gênero, nível de escolaridade, idade, hábitos de vida, identificação dos fatores de risco para as doenças crônicas não transmissíveis (DCNT) e apresentação de análises por região geográfica estão entre os resultados divulgados pelo Mapa desenvolvido por meio do SESI Viva+. Este é um exemplo dos trabalhos do SESI que buscam colaborar com o planejamento de ações que apoiem as indústrias.

38 SERVIÇO SOCIAL DA INDÚSTRIA –SENAI. **Transparência SESI**. 2023. Disponível em: https://www.portaldaindustria.com.br/sesi/canais/transparencia/. Acesso em: 21 jun. 2023.

39 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **Relato Integrado**. Brasília: SESI/DN, 2019. p. 15.

40 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **É no presente que o SESI constrói o futuro da educação e do trabalho**. 2023. Disponível em: https://www.portaldaindustria.com.br/sesi/institucional/. Acesso em: 21 jun. 2023; SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **Relato Integrado.** Brasília: SESI/DN, 2019. p. 82.

41 Documento disponível em: https://www.portaldaindustria.com.br/publicacoes/2022/6/mapa-da-saude-dos-trabalhadores-da-industria-atendidos-pelo-sesi-viva/.

42 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **Mapa da saúde dos trabalhadores da indústria atendidos pelo SESI Viva+**. Brasília: SESI/DN, 2021.

Nesse ínterim, observa-se que são tratados diversos dados pessoais referentes à identificação dos trabalhadores vinculados às empresas clientes do SESI (contratação direta), dependentes, menores aprendizes, associados ao nome, RG, CPF e data de nascimento. Além disso, há dados pessoais sensíveis, notadamente os relativos à saúde dos trabalhadores, como tipo sanguíneo, cor (raça) e nome social.

Os dados das empresas e trabalhadores são coletados pelos Departamentos Regionais, que irão atender o contrato celebrado com a empresa, mas também são transferidos para o Departamento Nacional atender à prestação de contas. Ademais, no âmbito da saúde ocupacional do trabalhador, o SESI dispõe de serviços médicos ocupacionais e exames ocupacionais, para consultas médicas admissionais, periódicas e demissionais, emissão de atestados de mudança de função e retorno ao trabalho.

No âmbito educacional, o SESI tem importante papel no desenvolvimento da educação básica do Brasil. A entidade atua na educação infantil, ensino fundamental e médio, além de promover a educação de jovens e adultos (EJA) e a educação continuada, específicos aos trabalhadores da indústria. No tocante às atividades de ensino, é possível destacar a necessidade de cuidado adicional dos dados de crianças e adolescentes, necessários para a realização de matrícula, cadastro dos alunos, identificação dos responsáveis, dados sobre eventual pessoa com deficiência (PcD) e desempenho escolar.

Na área da cultura, por sua vez, o SESI proporciona o desenvolvimento de novas metodologias que ensejam a interdisciplinaridade e o diálogo entre diferentes áreas de conhecimento, com medidas voltadas ao fortalecimento da arte brasileira nos níveis artístico e institucional. As principais ações executadas são o Programa Nacional de Acesso à Cultura; Ação Global e o Centro de Arte, Ciência e Tecnologia.[43]

5.1.4 IEL

O IEL, por meio de sua estrutura nacional, "estimula a autonomia dos Núcleos Regionais, que executam os projetos e desenvolvem novos negócios."[44] Em vista disso, dispõe de "soluções customizadas em gestão corporativa, educação empresarial e desenvolvimento de carreiras", atuando no aprimoramento da gestão e da educação empresarial, assim como agente de integração. Atualmente, conta com programas de estágio, oferta de serviços, como aperfeiçoamento da gestão, capacitação empresarial e consultorias para empresas dos mais diversos portes.

43 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **Relato Integrado**. Brasília: SESI/DN, 2019. p. 85.

44 IEL. **Estrutura**. 2023. Disponível em: https://www.portaldaindustria.com.br/iel/institucional/estrutura/. Acesso em: 21 jun. 2023.

Portanto, em sua estrutura, há o tratamento de dados pessoais para fins de gestão administrativa de contratos de estágio como agente integrador. Com tais fins, são ofertados serviços de Processo Seletivo, por meio do qual são selecionados previamente alunos, o que pode envolver entrevistas, testes psicológicos, avaliação de currículo e do histórico escolar atualizado. Nessa etapa, busca-se conciliar a formação do aluno com o perfil informado pela Unidade Concedente de Estágio.

Etapa posterior refere-se à Regularização, tal qual exigido por normas como a Lei nº 11.788/2008, conhecida como a Lei do estágio. Assim, há a emissão do Termo de Compromisso de Estágio (TCE), além de Termos Aditivos, registro do estágio na Carteira de Trabalho e Previdência Social (CTPS) do aluno e sua inclusão na apólice de seguro contra acidentes pessoais.

Outro serviço disponibilizado é o "Acompanhamento Avaliativo", que pode ocorrer com visitas periódicas agendadas entre os núcleos regionais e a Unidade Concedente de Estágio. De modo a viabilizar o acesso e compartilhamento dos dados, o IEL conta com sistemas próprios, a exemplo do Sistema Nacional de Estágio.

Vale observar que, diferentemente do que ocorre com SESI e SENAI, cada núcleo regional é uma pessoa jurídica distinta e autônoma "no que se refere à administração de seus serviços, gestão de seus recursos, regime de trabalho e relações empregatícias."[45] Assim, embora o cadastro dos candidatos ocorra por meio da base nacional de estágio do IEL, é possível, em razão da realidade de cada localidade, que a oferta e análise das candidaturas ocorram de modo diferente entre os núcleos. Ou seja, o processo avaliativo para vagas de estágio em Psicologia no Mato Grosso pode ser distinto do que ocorre no Ceará para vagas na área de Administração.

Da mesma forma, o IEL atua na concessão de bolsas para estudantes e egressos da academia desempenharem atividades específicas de educação executiva e gestão empresarial. Em seu ramo de desenvolvimento empresarial, as atividades destinam-se aos campos da (i) Educação Executiva e Empresarial, com atuação na "educação, de forma customizada, para a melhoria das competências em gestão das empresas"; (ii) Consultoria Empresarial, por meio de "projetos e consultorias para a promoção da inovação e para o aprimoramento das competências em gestão"; e (iii) Desenvolvimento de talentos, por meio da inserção de "jovens talentos nas empresas, desenvolvendo as competências requeridas para a atuação no mercado de trabalho."[46]

45 Art. 25, §1º do IEL. Núcleo Central. **Estatuto.** Brasília: IEL/NC, 2009. p. 20.

46 INSTITUTO EUVALDO LODI – IEL. **Desenvolvimento Empresarial (Educação, Consultoria e Desenvolvimento de Talentos)**. 2023. Disponível em: https://www.portaldaindustria.com.br/iel/institucional/estrutura/. Acesso em: 21 jun. 2023.

O IEL também organiza prêmios e concursos às categorias, como o Prêmio IEL de Estágio, voltado aos estagiários (categoria Projetos Inovadores), a quem representa uma empresa (Empresa Inovadora) ou a instituição de ensino (Educação Inovadora).[47] Com este fim, são utilizados dados relativos das empresas concorrentes (micro e pequenas, médias e grandes), estagiários, seus supervisores e Instituições de Ensino aos quais estão vinculados. Dessa maneira, os dados de inscrição, como a identificação das pessoas físicas e jurídicas, e sobre os quesitos avaliados acerca da inovação e impacto dos projetos inscritos são importantes para a concretização da iniciativa.

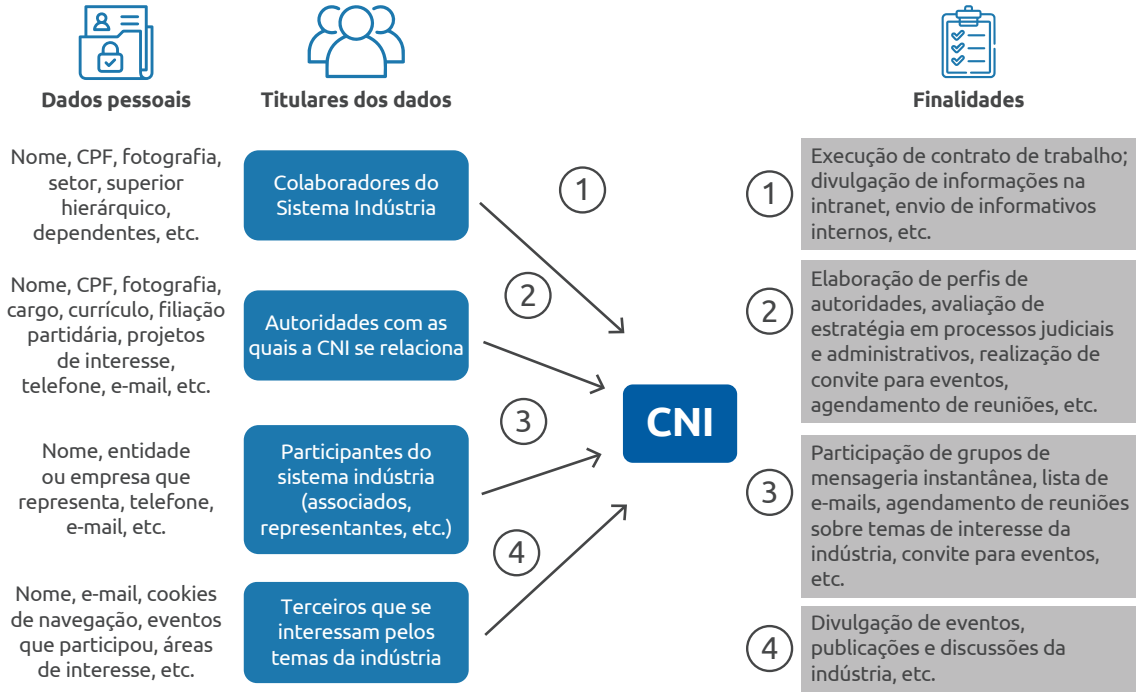
5.2 FLUXOGRAMA

Diante das considerações sobre os entes que compõem o Sistema Indústria, fica evidente que, internamente e entre cada um deles, há constante necessidade de troca de dados. Essa atividade é inevitável à própria gestão dos serviços prestados, como também para fins de auditoria, por exemplo, uma vez que as informações financeiras e ações desenvolvidas pelos departamentos nacionais e regionais de SESI e SENAI passam pelo crivo do Tribunal de Contas da União.

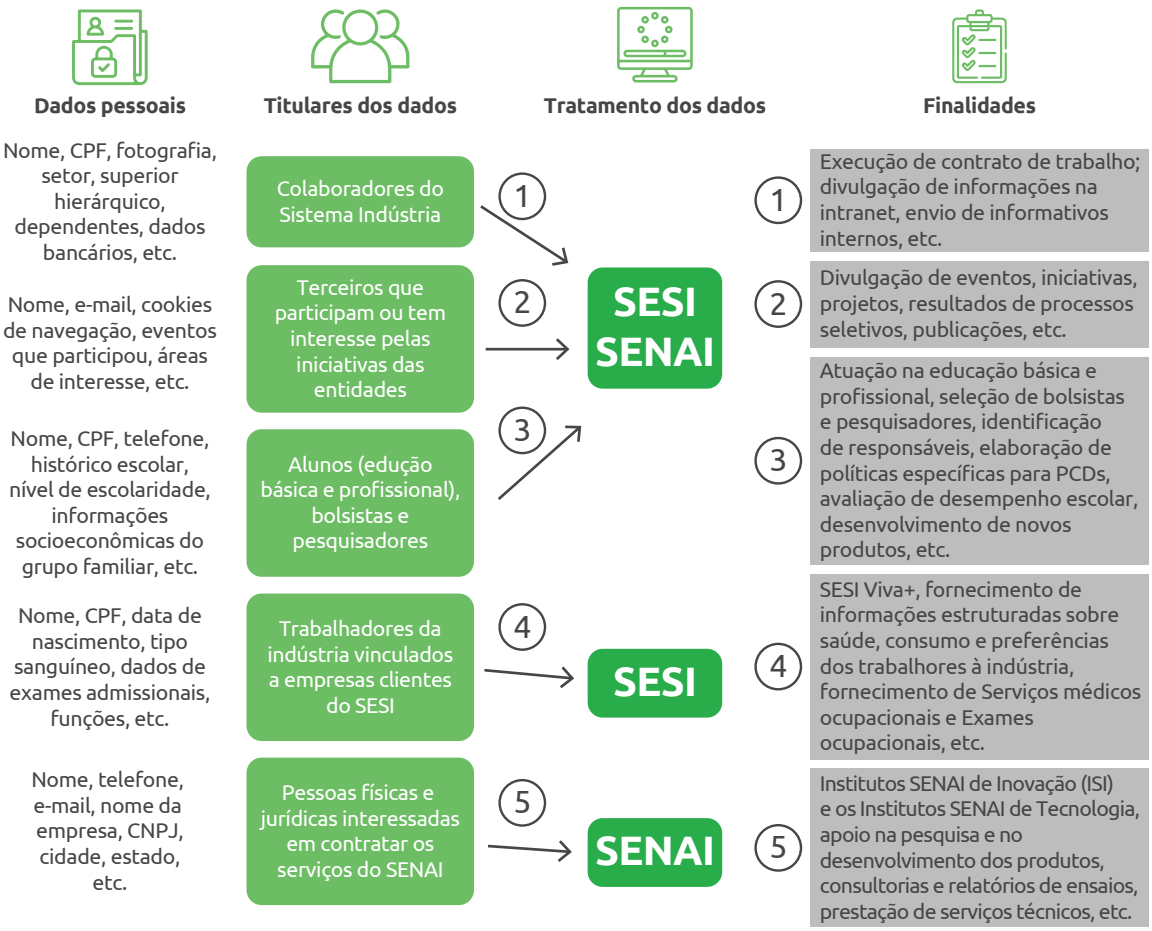
Portanto, o ciclo de vida dos dados pessoais no Sistema Indústria, ou em outras palavras, o fluxo de dados dentro dele tem grande complexidade. Consequentemente, o gerenciamento dos dados, observando os protocolos de segurança e período de retenção e exclusão dos dados, é um dos meios para que a adequação da LGPD seja materializada.

47 INSTITUTO EUVALDO LODI – IEL. **Prêmio IEL de Estágio 2022**. 2023. Disponível em: https://www.portaldaindustria.com.br/iel/canais/iel-estagio/premio-de-estagio. Acesso em: 21 jun. 2023.

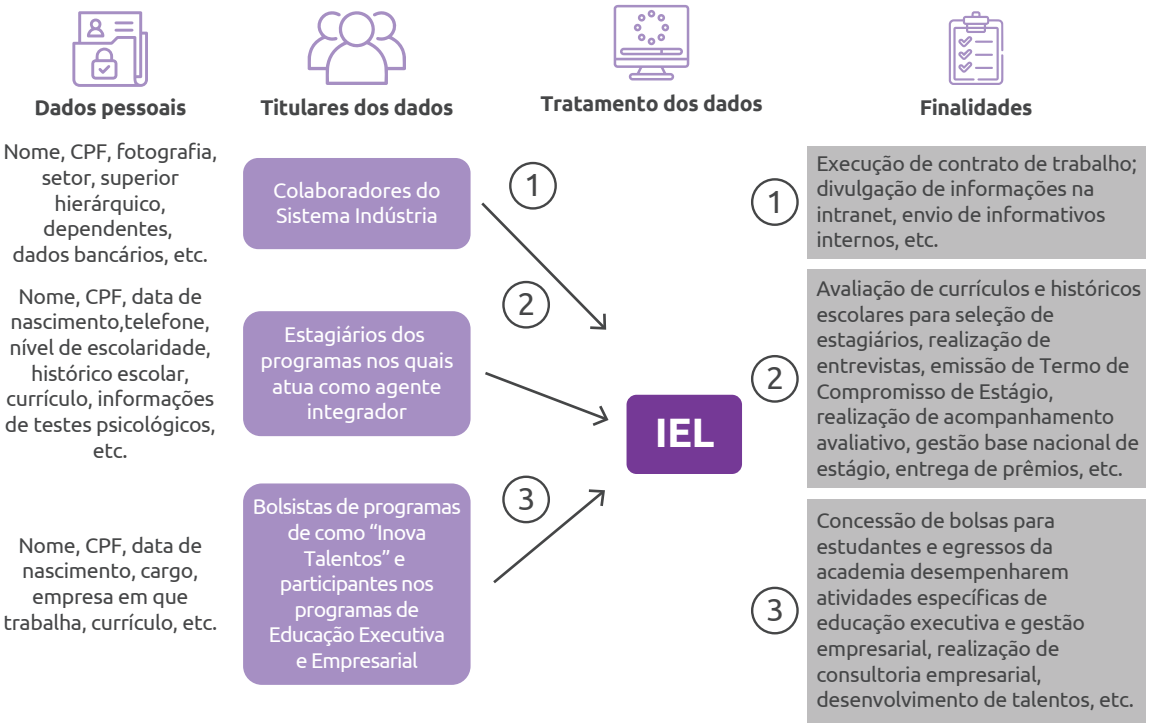
Fluxograma tratamento de dados CNI



Fluxograma tratamento de dados SESI e SENAI



Fluxograma tratamento de dados Sistema IEL



6 ÂMBITO DE APLICAÇÃO

Como apresentado no início do Guia de Boas Práticas, o objetivo é que as proposições de implementação da LGPD aqui fornecidas sejam destinadas ao Sistema Indústria em seu âmbito interno, abrangendo a sua atuação regional e nacional. Assim, o guia aplica-se às diferentes entidades autônomas, incluindo o sistema CNI, SENAI, SESI e IEL.

É certo que todas essas entidades compartilham desafios para a promoção da indústria, que exigem o constante tratamento de dados, conforme as características particulares de cada setor.

Dessa forma, os protocolos que serão apresentados nas Partes II e III buscam endereçar as principais demandas de cada entidade, contribuindo para que o tratamento de dados ocorra de forma legítima e em respeito ao direito fundamental de proteção de dados pessoais, estabelecido pela Constituição Federal.

PARTE 2

PROTOCOLOS GERAIS

1 PROTOCOLO PARA GARANTIA DOS DIREITOS DOS TITULARES

1.1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais define que os titulares de dados pessoais são qualquer pessoa natural a quem se referem os dados que são objeto de tratamento. A identificação dos sujeitos é passo importante para garantir que os seus direitos possam ser exercidos, como previsto nos termos dos arts. 9º, 18 e 20 da LGPD:

DIREITO DOS TITULARES

- Acesso facilitado a informações.
- Confirmação da existência de tratamento.
- Correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com regulamentação da ANPD, observados os segredos comercial e industrial.
- Eliminação dos dados pessoais tratados com o consentimento do titular, salvo exceções legais.
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- Revogação do consentimento.
- Oposição ao tratamento irregular.
- Revisão de decisões automatizadas.
- Petição perante a ANPD ou perante os organismos de defesa do consumidor.

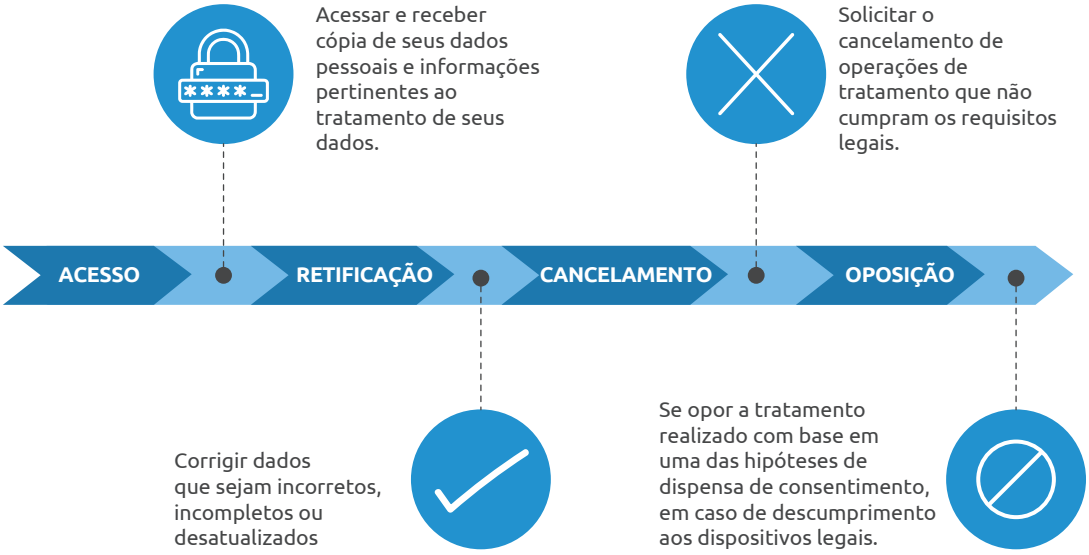
Nesse sentido, cabe indicar que a LGPD disciplina procedimentos voltados não apenas à garantia da proteção dos direitos dos titulares, como também assegura o seu exercício. Por isso, é importante adotar uma visão holística sobre a proteção e exercício dos direitos dos titulares, pois estes partem da LGPD, mas não se limitam a esta norma porque outras leis do direito brasileiro podem ser aplicadas ao caso.

É notável que os direitos dos titulares estejam intimamente atrelados às atividades que devem ser desempenhadas pelos agentes de tratamento e encarregados pela proteção de dados pessoais, uma vez que são responsáveis por garantir que as normas e os princípios estabelecidos pela LGPD sejam respeitados nas instituições e funcionem como pontos de referência para os titulares. Desse entendimento, destaca-se o papel do encarregado, que centraliza o recebimento de dúvidas e solicitações, sendo estratégico no relacionamento com os titulares e no aumento da confiança deles sobre os dados que são tratados.

Assim, é de grande importância que todas as entidades e órgãos do Sistema Indústria disponibilizem os contatos dos encarregados, de preferência no respectivo sítio eletrônico (art. 41, §1º, da LGPD).

1.2 ASSEGURANDO OS DIREITOS DOS TITULARES – ARCO

Entre os direitos dos titulares previstos na legislação, merece atenção especial os direitos de acesso, retificação, cancelamento e oposição, representados pelo acrônimo ARCO.



O direito de **acesso** possui relação com os princípios do livre acesso, transparência e prestação de contas, e a recusa em prestar as informações solicitadas deve ocorrer apenas em situações fundamentadas. Já o direito de **retificação** refere-se à possibilidade de os titulares corrigirem dados que estejam incorretos, incompletos ou desatualizados.

Associa-se esse direito ao princípio da qualidade dos dados e do livre acesso previsto no art. 6º, V, da LGPD, uma vez que os dados dos titulares devem ser exatos, atualizados, claros e relevantes.

Por sua vez, o direito de **cancelamento** (ou eliminação) refere-se à opção do titular solicitar que determinados dados não sejam tratados e, portanto, sejam excluídos. Por fim, o direito de **oposição** previsto pelo art. 18, §2º[48] da LGPD possibilita que os titulares dos dados pessoais se oponham a situações de tratamento nas hipóteses de dispensa de consentimento, caso seja comprovado o descumprimento aos dispositivos legais.

48 "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei".

Recomenda-se que as entidades definam protocolos e prazos internos para que as solicitações dos titulares sejam atendidas em tempo hábil. A LGPD dispõe, em seu art. 19, o prazo para envio de declaração completa para confirmação de existência ou acesso a dados pessoais em até 15 (quinze) dias (inciso II) ou, imediatamente, em formato simplificado (inciso I). Em relação aos demais direitos dos titulares, a ANPD, ainda, não se manifestou sobre a sua definição, mas deve fazer futuramente.

Dessa forma, será respeitado o período necessário para que as medidas sejam avaliadas e providenciadas com segurança, uma vez que os pedidos podem ser recusados apenas em hipóteses excepcionais.

Para que os direitos dos titulares sejam operacionalizados e respeitados pelas entidades, recomendam-se algumas medidas para ações ágeis que respeitem a cautela necessária ao se tratar dados pessoais. São elas:

- Definir as hipóteses de incidência para cada direito do titular.
- Determinar quais serão as formas seguras de identificação dos titulares de dados, como redução de riscos para que terceiros alterem ou solicitem modificações de dados sem autorização.
- Registrar a data do recebimento do pedido.
- Definir fluxos internos para as situações de solicitação de exercício dos direitos e meios para identificar um pedido de informação.
- Definir prazos para atender aos pedidos de informação e às hipóteses de interrupção do prazo, se forem necessárias informações adicionais que impeçam o atendimento do pedido.[49]
- Identificar se foi dado o consentimento para o tratamento do dado.
- Identificar quando um pedido de informação pode envolver informações de outros titulares.
- Possuir procedimentos para informar outros agentes de tratamento com quem o dado tenha sido compartilhado sobre eventual cancelamento, que também deverá ser adotado pelos outros agentes.
- Quando o tratamento tiver origem no consentimento do titular ou em contrato, providenciar o acesso do titular à cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
- Fornecer informações claras e adequadas acerca da origem dos dados, a inexistência de registro, os critérios utilizados para o tratamento de dados e a finalidade do tratamento, observados os segredos comercial e industrial ao atender aos pedidos do titular.
- Possuir sistemas de gerenciamento de informações eficientes que permitam o cancelamento das informações e sua eliminação.
- Identificar se os dados solicitados são pertinentes e informar, pelo menos:
  a. finalidade específica do tratamento;
  b. forma e duração do tratamento, observados os segredos comercial e industrial;
  c. identificação do controlador;
  d. informações de contato do controlador;
  e. informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
  f. responsabilidades dos agentes que realizarão o tratamento; e
  g. direitos do titular especificados no art. 18 da LGPD.

49 Em observância ao art. 19 da LGPD que fixa o limite de 15 (quinze) dias de resposta ao titular após o seu requerimento.

Acrescenta-se às recomendações anteriores a importância de que as entidades disponham de procedimentos que informem os demais operadores de dados do Sistema Indústria que, em nome do controlador, realizam o tratamento de dados.

Como restou comprovado na Parte I deste guia, o fluxo de compartilhamento de dados dentro do Sistema Indústria é alto e a efetivação do cumprimento à LGPD requer clareza desse processo, para tornar o atendimento aos direitos dos titulares mais eficiente. Assim, recomendamos que o atendimento do direito dos titulares tenha como princípio norteador o da transparência, garantindo que os titulares tenham acesso a informações claras, precisas e facilmente acessíveis, respeitados os segredos comercial e industrial.

A implementação desse princípio pode se dar por meio de políticas de privacidade ou mesmo painéis de controle por meio do qual os usuários possam controlar suas preferências e acessar informações. Entre as informações que devem ser disponibilizadas para o titular estão:[50]

Conteúdo das políticas de privacidade

- Principais formas de coleta dos dados pessoais.
- Operações de tratamento de dados realizadas.
- Finalidades do tratamento de dados do titular.
- Informações sobre compartilhamento de dados (dados compartilhados e com quem).
- Caso dados sejam coletados de outras fontes e não seja fornecido diretamente pelo titular, publicar quais categorias de dados são coletadas.
- Principais bases legais utilizadas no tratamento de dados.
- Informações sobre a transferência internacional de dados.
- Informações sobre a existência de obrigações legais que exigem o compartilhamento de dados.
- Informações sobre a utilização de decisões automatizadas, perfilamento e rastreamento.
- Dados para contato com o DPO.
- Caso a política de privacidade seja alterada, disponibilizar avisos e garantir que tal informação seja amplamente difundida, com prazo razoável entre o aviso e a efetiva implementação das mudanças.
  - Caso se trate de tratamento de dados de colaboradores, disponibilizar avisos internos sobre a alteração.

50 Essa lista foi elaborada com base nos seguintes *checklists*: INFORMATION COMISSIONER'S OFFICE – ICO. **Right to be informed**. 2023. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. Acesso em: 21 jun. 2023; CNSAÚDE. **Código de boas práticas**: proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 21 jun. 2023; CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. No prelo.

1.3 ATENDIMENTO AOS DIREITOS DOS TITULARES DE DADOS QUE SÃO COLABORADORES DO SISTEMA INDÚSTRIA

Para garantir o direito dos titulares que já são colaboradores do Sistema Indústria, algumas medidas podem ser adotadas para otimizar o atendimento em relação aos titulares que são externos ao Sistema. Isso porque, adotando procedimentos distintos para cada "categoria" de titulares, o atendimento ao público geral pode ser mais eficiente.

Por exemplo, para atendimento dos direitos dos titulares do público interno do Sistema Indústria, que envolve os colaboradores, recomendamos a inclusão de sistema que possibilite a gestão de informações na intranet. A intranet do Sistema Indústria já possui diversas finalidades como atualização de dados e acesso a informações cadastrais, mas pode ser ampliada para compreender a gestão de outras informações como a possibilidade de não deixar pública a data de aniversário dos colaboradores.

Contudo, também, recomendamos que seja incluída a possibilidade de o colaborador definir se deseja, por exemplo, divulgar sua data de nascimento e foto para todos os outros colaboradores. Ou então, é possível solicitar o consentimento dos colaboradores para outras ações, como é o caso de utilização de imagem para divulgação de ações ou eventos –, assim como também é possível utilizar o sistema para o gerenciamento do consentimento fornecido.

Notadamente, dados que sejam centrais para o atendimento de finalidades da relação de trabalho do colaborador ou que sejam necessários para o atendimento de obrigações legais, como no caso de dados cadastrais como o vínculo de emprego, não devem ser facilmente alterados pelos colaboradores nos sistemas internos. Ainda assim, os sistemas podem ser utilizados para possibilitar o acesso dos colaboradores aos dados armazenados, ainda que sua modificação não seja possível.

Importa notar que também pode ser disponibilizada uma política de privacidade específica para os colaboradores, com um canal específico para atendimento aos seus direitos, como é o caso da Ouvidoria que foi criada para a comunicação dos colaboradores em casos de infrações ao Código de Ética do Sistema Indústria.[51]

51 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI; SERVIÇO SOCIAL DA INDÚSTRIA – SESI; SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI; INSTITUTO EUVALDO LODI –IEL. **Código de Conduta Ética**. Brasília: CNI, 2021.

2 PROTOCOLO PARA ARMAZENAMENTO, COMPARTILHAMENTO INTERNO E ELIMINAÇÃO DE DADOS

2.1 INTRODUÇÃO

A adequação dos processos à LGPD é um dos fatores que auxiliam no cumprimento das missões institucionais de cada representante do Sistema Indústria, razão pela qual é imprescindível considerar o fluxo de dados e especificidades de cada entidade ou órgão.

Nesse sentido, o *checklist* elaborado pelo CIPL, em parceria com o Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP), ressalta quais são as prioridades para as organizações, públicas e privadas, implementarem de forma eficaz a LGPD"[52]:

CHECKLIST: ETAPAS PRIORITÁRIAS PARA A ADEQUAÇÃO À LGPD

Prioridade 1. Entender o impacto da LGPD na organização e obter a adesão da alta administração

- ☑ Compreender o impacto das regras da LGPD na organização e o uso de dados pessoais como controlador e/ou operador.
- ☑ Explicar e demonstrar à alta administração a importância da adequação às regras de privacidade e os benefícios da prestação de contas.
- ☑ Solicitar apoio da alta administração, incluindo para orçamento e recursos.

Prioridade 2. Designar o encarregado pelo tratamento de dados pessoais, e identificar e envolver os principais *stakeholders*

- ☑ Designar o encarregado, documentar e comunicar internamente seu papel e suas responsabilidades.
- ☑ Identificar e envolver os principais *stakeholders* internos e líderes sêniores que patrocinarão o programa de governança de privacidade e proteção de dados pessoais e terão responsabilidade pela implementação do programa.
- ☑ Identificar e envolver os principais *stakeholders* externos.

52 CIPL; CEDIS-IDP. **Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD).** Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[pt]_cipl-idp_white_paper_on_top_priorities_for_organizations_to__effectively_implement_the_lgpd_7_october_2020_.pdf. Acesso em: 04 jul. 2022.

Prioridade 3. Identificar as atividades de tratamento e os dados utilizados pela organização

- ☑ Definir a metodologia para mapear e registrar as atividades de tratamento de dados pessoais efetuadas pela organização (como controladora e/ou operadora) e revisar periodicamente o ciclo de vida dos dados.
- ☑ Mapear os dados pessoais e as respectivas atividades de tratamento o mais rápido possível.
- ☑ Considerar a anonimização e minimização de dados para reduzir os riscos e o ônus decorrente da obrigação de conformidade da organização.

Prioridade 4. Determinar o papel e as obrigações da organização ao atuar como controladora ou operadora

- ☑ Determinar o papel e as obrigações da organização como controladora ou operadora.
- ☑ Comunicar essas obrigações aos indivíduos e às equipes relevantes dentro da organização.
- ☑ Considerar atualizações necessárias aos contratos dos clientes para refletir o papel da organização.

Prioridade 5. Avaliar os riscos associados ao tratamento de dados pessoais

- ☑ Implementar processo de avaliação de riscos aos indivíduos relacionados ao tratamento de dados pessoais.
- ☑ Priorizar as medidas de conformidade relacionadas ao tratamento de dados pessoais que implicam maiores riscos para os indivíduos e para a organização.

Prioridade 6. Elaborar e implementar um programa de governança de privacidade e proteção de dados pessoais que cubra as exigências da LGPD

- ☑ Elaborar um programa de governança de privacidade e proteção de dados pessoais e um plano de ação para implementá-lo com base nos riscos identificados.
- ☑ Identificar quais são as ações mais simples e implementá-las o mais rápido possível.
- ☑ Manter e revisar o programa de governança de privacidade e proteção de dados pessoais de forma contínua.

Prioridade 7. Definir as bases legais para as atividades de tratamento de dados da organização

- ☑ Identificar os indivíduos ou equipes que serão responsáveis por determinar as bases legais para o tratamento de dados pessoais – esses indivíduos deverão, como prioridade, definir em quais bases legais a organização se baseará.
- ☑ Considerar quais processos devem ser implementados e/ou adaptados para a manutenção contínua das bases legais.

Prioridade 8. Definir medidas técnicas e administrativas para garantir a segurança dos dados pessoais, assim como para elaborar relatórios internos e gerenciamento efetivos de incidentes de segurança

- ☑ Trabalhar com as equipes de segurança da informação e de arquitetura de sistemas/dados para determinar as mudanças necessárias para implementar as medidas apropriadas de segurança.
- ☑ Estabelecer um processo para a elaboração de relatórios internos, gerenciamento de incidentes de segurança, violações de dados pessoais e notificação da ANPD, se necessário.

Prioridade 9. Identificar os terceiros com os quais a organização compartilha dados pessoais e estabelecer um processo de gestão de terceiros

- ☑ Identificar os terceiros que realizam tratamento de dados pessoais em nome da organização e determinar se a organização trata dados pessoais em nome de terceiros.
- ☑ Avaliar e adotar mecanismos de gerenciamento de terceiros, incluindo processos de *due diligence* e a celebração de contratos relacionados ao tratamento de dados.

Prioridade 10. Identificar os fluxos internacionais de dados da organização (entrada e saída) e estabelecer os mecanismos apropriados para permitir tal transferência de dados

- ☑ Identificar se a organização transfere dados pessoais para outros países e, se o faz, para quais finalidades e em qual capacidade (como controlador ou como operador).
- ☑ Avaliar e implementar os mecanismos de transferência de dados mais apropriados.

Prioridade 11. Construir processos eficazes para transparência e gerenciamento dos direitos dos titulares de dados pessoais

- ☑ Preparar avisos de privacidade e outros recursos para fornecer informações facilmente acessíveis aos titulares de dados sobre o tratamento realizado pela organização.
- ☑ Mapear os possíveis casos de exercícios de direitos pelos titulares relacionados aos seus dados pessoais, avaliar o tempo que a organização precisaria para responder e para desenvolver os processos relevantes.
- ☑ Desenvolver processos para responder a tais solicitações.

Prioridade 12. Treinar funcionários sobre as regras da LGPD e criar um programa de conscientização

- ☑ Implementar treinamento contínuo para todos os funcionários, incluindo os terceirizados e os recém-chegados.
- ☑ Planejar atividades de treinamento e comunicação tanto no início do programa de governança de privacidade e proteção de dados pessoais quanto de forma contínua.

Ao serem implementadas as 12 prioridades anteriormente elencadas, verifica-se que o aspecto fundamental para o cumprimento com a LGPD é a clareza acerca do fluxo de dados de cada entidade ou órgão, que envolve atividades de tratamento como a coleta (captação, produção e recepção dos dados), retenção (por meio do armazenamento e arquivamento), processamento (que pode ocorrer pela reprodução, avaliação e modificação), compartilhamento (voltado à distribuição e transferência dos dados, por exemplo) e eliminação (com o fim do tratamento de dados).

Esse fluxo dos dados foi apresentado na Parte I deste guia na forma do seguinte fluxo simplificado:

Assim, para abordar as principais preocupações envolvidas ao longo do ciclo de vida dos dados pessoais em uma instituição, serão endereçadas três modalidades de tratamento: o armazenamento, o compartilhamento interno e a eliminação. Essas são etapas sensíveis, pois envolvem a forma em que os dados são gerenciados internamente na organização e uma avaliação minuciosa acerca da necessidade de excluí-los quando atingida a finalidade para a qual eles foram coletados, bem como as determinações legais e regulatórias que justificam o seu armazenamento na organização.[53]

Essas etapas exigem um grau elevado de amadurecimento das entidades e órgãos, de conhecimento acerca dos dados que são tratados, finalidade do tratamento de dados, assim como as medidas de segurança que devem ser adotadas quando do armazenamento dos dados pessoais.

Por esse motivo, o princípio da necessidade é fundamental nessa etapa, na medida em que estabelece que os dados devem ser tratados para as finalidades legais para as quais foram coletados.

2.2 ARMAZENAMENTO DOS DADOS

As entidades e os órgãos integrantes do Sistema Indústria devem dispor de revisões periódicas sobre a qualidade e necessidade de os dados serem mantidos, uma vez que os dados pessoais podem ficar armazenados por um longo período de tempo. Para auxiliar nessa avaliação, algumas questões podem orientar a avaliação sobre a adequada aplicação dos princípios:

- Todos os dados pessoais que irei coletar são necessários para atingir a finalidade para a qual eles serão utilizados?
- Existe uma forma menos invasiva de tratar esses dados?
- Eu irei violar algum direito do titular com a minha operação de tratamento de dados?
- Existe o potencial de restrição a direitos ou liberdades com a operação de tratamento que irei realizar?
- O titular foi informado sobre os usos que farei dos dados?
- Eu consigo possibilitar o acesso do titular a informações sobre seus dados pessoais?
- Onde e como irei guardar os dados?
- Os dados que estou tratando estão seguros?
- A finalidade que eu inicialmente estabeleci foi finalizada? Eu ainda preciso de todos os dados que coletei inicialmente?
- A finalidade inicial se alterou ao longo do tratamento?

53 É o que define as melhores práticas internacionais. Nesse sentido, recomenda-se: INFORMATION COMISSIONER'S OFFICE – ICO. **Principle**: storage limitation. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/. Acesso em: 24 ago. 2022; EUROPEAN COMMISSION. **For how long can data be kept and is it necessary to update ir?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/howlong-can-data-be-kept-and-it-necessary-update-it_en. Acesso em: 24 ago. 2022.

Aqui, as entidades e os órgãos do Sistema Indústria possuem importante papel no estabelecimento de metas e prazos internos de revisões conjuntas aos demais participantes, para que essa atividade seja regularizada e habitual. Atende-se, portanto, ao princípio da minimização, para que os dados sejam retidos na medida em que forem necessários, adequados e restritos aos fins pelos quais são processados. Ademais, deve-se garantir que os outros princípios da LGPD também sejam observados ao longo de todo o período:

- A entidade deve saber quais dados possui, por quanto tempo eles serão necessários ou para qual(is) finalidade(s), devendo o agente de tratamento ser capaz de apresentar uma justificativa para o seu armazenamento (**PRINCÍPIO DA FINALIDADE E PRESTAÇÃO DE CONTAS – arts. 6º, I e X, da LGPD**).
- É necessário garantir que o tratamento de dados tenha como finalidade propósitos legítimos, específicos e explícitos em todo o ciclo de vida dos dados coletados – ou seja, de forma contínua –, não sendo possível armazenar um dado sem que exista um objetivo claro para tanto **(PRINCÍPIO DA FINALIDADE – art. 6º, I, da LGPD**).
- Com o acompanhamento permanente das atividades de tratamento de dados será possível tomar decisões sobre quando determinados dados não precisam mais ser coletados ou devem ser excluídos por não serem mais necessários (**PRINCÍPIO DA NECESSIDADE – art. 6º, III, da LGPD**).
- Por vezes, nem todos os dados coletados inicialmente são necessários, devendo a sua utilização ser minimizada ao máximo, inclusive, por meio da anonimização ou pseudonimização quando possível (**PRINCÍPIO DA NECESSIDADE – art. 6º, III, da LGPD**).
- Caso a finalidade se altere ao longo do período de tratamento e não seja possível excluí-lo, devem ser adotadas medidas para que o titular seja informado ou possa acessar informações sobre a mudança de finalidade (**PRINCÍPIO DA ADEQUAÇÃO E DA TRANSPARÊNCIA – art. 6º, II e VI, da LGPD)**.
- É necessário garantir que o dado armazenado esteja atualizado e é fidedigno após um longo período de armazenamento. Caso não seja possível identificar se ele está correto, pedir a atualização do dado para o titular e reavaliar a necessidade do armazenamento desse dado. Ex. Telefone e endereço são dados que podem ficar desatualizados com rapidez, avaliar se após longo período eles ainda são necessários (**PRINCÍPIO DA NECESSIDADE E DA QUALIDADE DOS DADOS art. 6º, III e V, da LGPD**).

Atenção especial, nesse sentido, para as leis brasileiras e disposições setoriais que tornam o armazenamento de dados pessoais obrigatório. Como exemplo, podemos mencionar as inúmeras previsões das legislações trabalhistas, os prazos previstos no Código Civil sobre prescrição (arts. 205 e 206, exemplificativamente), assim como obrigações tributárias que fazem com que, por vezes, os dados tenham que ser armazenados por um período mais longo do que o estabelecido para a finalidade primordial para a qual o dado foi coletado.

Outro aspecto que merece atenção quando do armazenamento de dados pessoais envolve os avisos de privacidade, que devem ser revisados constantemente, deixando claras as finalidades para as quais os dados serão utilizados e hipóteses de retenção por um período mais longo.

De acordo com o art. 16 da LGPD, os dados podem ser mantidos após o término da finalidade pretendida para:

- cumprimento de obrigação legal ou regulatória pelo controlador (inciso I);
- realização de estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (inciso II);
- transferência dos dados a terceiro, desde que respeitados os requisitos de tratamento estabelecidos na LGPD (inciso III); e
- uso exclusivo do controlador, sendo proibido seu acesso por terceiro, e desde que anonimizados os dados (inciso IV).

Aqui, é incentivado que os colaboradores e, em especial, os agentes de tratamento de dados (controlador e operador) possam ter uma visão crítica para que os tratamentos de dados desempenhados sejam avaliados e saber se efetivamente estão de acordo com os compromissos firmados à época de produto ou projeto executado, promovendo uma cultura de proteção de dados a todos os níveis.

Ademais, outro aspecto importante sobre o armazenamento de dados pessoais se refere aos sistemas em que os dados são arquivados. Isso porque, caso os servidores estejam localizados fora do território brasileiro, por exemplo, seria a hipótese de transferência internacional dos dados. Nesse sentido, é importante manter o registro das operações de tratamento atualizado, mapeando todos os dados e finalidades que são tratados pelas entidades, além de criar tabelas de temporalidade e políticas de retenção abordando informações como:

• Dados armazenados.
• Prazo de guarda.
• Finalidade.
• Trata-se de cumprimento de obrigação legal ou regulatória?
– Qual norma subsidia a obrigação?
• Trata-se de exercício regular de direitos?
– Quais normas e prazos prescricionais foram considerados?
• Onde o dado está armazenado?

Caso os dados tenham que ser armazenados para o cumprimento de uma obrigação legal ou regulatória, avaliar a possibilidade de exclusão de, ao menos, parte dos dados a eles associados – em especial os dados sensíveis – e de pseudonimizar as informações. Por exemplo, caso seja necessário armazenar os documentos referentes ao recolhimento do Fundo de Garantia do Tempo de Serviço (FGTS) por 30 anos, dado o prazo prescricional

para a cobrança de valores não pagos,[54] não necessariamente os dados relativos ao estado civil do colaborador devem ser armazenados.

Assim, mesmo que parte das informações sobre determinado titular seja necessária, as entidades podem proceder com a exclusão parcial dos seus dados pessoais. Ademais, uma vez que essas informações não precisarão ser acessadas de forma constante por outros setores, elas podem ser pseudonimizadas para reduzir o risco de identificação em caso de um incidente de segurança, bem como devem ser adotadas medidas de segurança para evitar seu acesso indevido.

2.3 COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS NACIONAIS E REGIONAIS DO SISTEMA INDÚSTRIA

CNI e federações Estatuais e do Distrito Federal, núcleos nacional e regionais do IEL, assim como os departamentos regionais e nacionais do SENAI e SESI, por diversas vezes, necessitam compartilhar os dados entre si para operacionalização e gestão dos serviços prestados, cumprindo com as disposições regimentais de cada entidade e com as obrigações regulatórias as quais são submetidos, conforme será apresentando a seguir.

A transferência de dados entre os órgãos do SESI e do SENAI decorre, principalmente, da existência de mecanismos de fiscalização e auditoria que controlam o recebimento dos recursos advindos das contribuições compulsórias pelas entidades que integram os Serviços Sociais Autônomos – conforme previsto no parágrafo único do art. 70 da Constituição Federal. O processo de fiscalização dos recursos requer o acompanhamento acerca do cumprimento de acordo com as finalidades para as quais eles foram destinados.

Assim, considerando a existência de diversas normas específicas que versam sobre os procedimentos de controle, prestação de contas e integração dos órgãos nacionais e regionais, o compartilhamento de dados entre os órgãos pode ser justificado pelo cumprimento de obrigações legais nos termos do art. 7º, II, e 11, II, a, da LGPD.

O compartilhamento de dados dentro do Sistema também pode ser necessário para a elaboração de estudos e realização de levantamento de dados estatísticos que demonstrem a efetividade das iniciativas desenvolvidas por cada órgão e a efetiva execução de programas, como é o caso da concessão de bolsas. Em geral, esse compartilhamento de

54 BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário com Agravo 709.212 Distrito Federal**. Recurso extraordinário. Direito do Trabalho. Fundo de Garantia por Tempo de Serviço (FGTS). Cobrança de valores não pagos. Prazo prescricional. Prescrição quinquenal. Art. 7º, XXIX, da Constituição. Superação de entendimento anterior sobre prescrição trintenária. Inconstitucionalidade dos arts. 23, § 5º, da Lei 8.036/1990 e 55 do Regulamento do FGTS aprovado pelo Decreto 99.684/1990. Segurança jurídica. Necessidade de modulação dos efeitos da decisão. Art. 27 da Lei 9.868/1999. Declaração de inconstitucionalidade com efeitos *ex nunc*. Recurso extraordinário a que se nega provimento. Relator: Gilmar Mendes, Data de Julgamento: 25/10/2012, Tribunal Pleno. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=7780004. Acesso em: 27 maio 2023.

dados é solicitado pelas entidades. Nesse caso, sugere-se que, sempre que possível, sejam compartilhados dados anonimizados ou pseudonimizados.

O Regulamento do Serviço Social da Indústria (Decreto nº 57.375/65), por exemplo, dispõe que o Departamento Nacional tem como obrigação prestar contas e apresentar relatórios anuais ao Conselho Nacional (art. 33 do Regulamento do SESI). Assim, o compartilhamento de dados entre os Departamentos Regionais e o Departamento Nacional e pode ser realizado para essa finalidade.

Ademais, o SENAI, SESI e o IEL, contam com a Superintendência de Controle e Gestão. Para que suas atividades sejam desempenhadas, são compartilhados dados nacionais de educação, saúde e segurança na indústria. Nessa repartição são tratados dados dos seguintes atores:

a) Alunos matriculados em alguma das unidades por meio do qual o respectivo Departamento Regional do SENAI e SESI envia os dados cadastrais para a Superintendência por meio dos sistemas de cada entidade, para que a área realize a tratativa dos dados.
b) Clientes (pessoa física e pessoas físicas vinculadas a pessoas jurídicas) de ações de Educação, Saúde e Segurança, Cultura e Cooperação Social.
c) Funcionários, corpo docente e dados dos responsáveis pelas unidades operacionais: emissão de relatórios dos dados por meio do compartilhamento dos Departamentos Regionais para disponibilização de dados de infraestrutura e Recursos Humanos do SESI, do SENAI e do IEL.

Para tanto, tem-se, para tais atividades, bases legais distintas. Parte das operações de tratamento será realizada para execução do contrato, especialmente no momento da coleta inicial dos dados pelo departamento regional. Já a incidência de cumprimento de obrigação legal ou regulatória pode ser aplicável para operações como a prestação de contas sobre preenchimento de vagas gratuitas na área da educação e compartilhamento de dados pessoais com órgãos fiscalizadores, que é feito no âmbito dos departamentos nacionais. O legítimo interesse do controlador está relacionado à produção de relatórios, consolidação de estatísticas e acompanhamento dos indicadores para aperfeiçoamento das atividades, desde que não estejam envolvidos dados pessoais sensíveis.

Caso seja indispensável o tratamento de dados pessoais sensíveis, recomendamos a elaboração e revisão de documentos como RIPD, assim como a anonimização e pseudonimização das informações sempre que possível. Ademais, a utilização da base legal do consentimento também pode amparar o tratamento dessa modalidade de dados, sempre que forem atendidos os seus requisitos de validade (Protocolo Geral VIII.5., a.).

Ressalta-se que não é recomendável o uso da base legal do consentimento para as hipóteses de coleta de dados dos colaboradores pela própria instituição em que possuem algum vínculo de trabalho ou prestação de serviço. Isso porque o embasamento legal é fragilizado já que dificilmente é possível garantir que o colaborador concorde, *de forma livre, informada e inequívoca*, com o tratamento de seus dados pessoais quando quem os solicita possui relação profissional de nível hierárquico superior.

Uma das principais críticas ao uso da base legal do consentimento em relações trabalhistas refere-se ao reconhecimento do desequilíbrio entre as partes, uma vez que existe uma relação de poder entre patrão e trabalhador que impossibilita que o consentimento seja *livre*. Da mesma forma, a qualquer momento, o titular dos dados pessoais pode solicitar a revogação de seu consentimento, fato que pode prejudicar o desenvolvimento das atividades do controlador.

Ainda nesse sentido é que se tem a manifestação do Grupo de Trabalho do Artigo 29 (GT29),[55] em seu Considerando nº 43, ao reconhecer como problemática a possibilidade de o consentimento não ser fornecido de forma livre:

> **Considerando nº 43.** A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa.
>
> Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.[56]

A interação e o compartilhamento de dados entre o Departamento Nacional e os Departamentos Regionais também podem ocorrer no bojo das atividades de Telemedicina, SESI Facilita e Info SESI no âmbito do SESI. Este é um sistema de gestão de saúde e segurança no trabalho, mantido pelo Departamento Nacional e fornecido para as empresas clientes, Departamentos Regionais e unidades operacionais do SESI. Na prestação de serviços de telemedicina, por exemplo, os dados das empresas e trabalhadores são coletados pelas unidades operacionais ou pelos Departamentos Regionais, que irão atender o contrato celebrado com a empresa.

55 "O Grupo de Trabalho do Artigo 29 (GT Art. 29) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD)." Disponível em: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_pt.

56 Tradução disponível em: https://gdpr-text.com/pt/read/recital-43/.

Tais dados sensíveis podem ser tratados pelo profissional de saúde por meio da base legal tutela da saúde (art. 11, II, f, LGPD) ou por outros agentes mediante coleta do consentimento (art. 11, I, LGPD) ou cumprimento de obrigações legais (11, II, a LGPD). Ainda assim, por se tratarem de dados pessoais sensíveis é necessário cuidado adicional com o controle de acesso às informações, e com a avaliação da finalidade do compartilhamento dos dados. Dessa forma, mesmo que os dados possam ser compartilhados, a minimização dos dados disponibilizados e a pseudonimização das informações é medida essencial.

Por fim, insta ressaltar que o compartilhamento de dados pessoais entre as entidades e órgãos no âmbito nacional e regional não deve ocorrer de forma indiscriminada, abrangendo todo e qualquer dado. Assim, além das normas que viabilizam a estrutura e funcionamento das entidades do Sistema Indústria, devem ser observados os princípios da LGPD, em especial o da necessidade, finalidade e adequação ao contexto do tratamento. Ademais, deve-se garantir que o mínimo de dados necessários seja tratado, para que o compartilhamento ocorra, anonimizando ou pseudonimizando, os dados pessoais sempre que possível.

2.4 ELIMINAÇÃO DOS DADOS PESSOAIS

Conforme determinação da LGPD, o término do tratamento de dados deve ocorrer quando: i) a finalidade for alcançada ou os dados não forem mais necessários; ii) o período do tratamento tiver terminado; iii) o titular tiver revogado seu consentimento; e iv) a Autoridade Nacional determinar o término do tratamento por conta de violação à lei (art. 15 da LGPD).

A *eliminação* é uma modalidade de tratamento de dados pela qual há a exclusão de dados ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento utilizado. Logo, a definição das finalidades para o tratamento e do tempo necessário para que sejam mantidos é algo importante para a orientação da eliminação das informações.

Também cabe relembrar que a LGPD abrange os dados pessoais independentemente do meio em que estão, se no formato físico ou virtual. No meio físico, deve-se ter cautela quanto aos formatos de descarte, evitando-se que papéis sejam descartados integralmente. Recomenda-se que as informações pessoais sejam rasuradas e os documentos triturados, por meio de protocolos que confirmem que tal processo ocorreu validamente.

Também podem ser contratadas empresas especializadas para a eliminação das informações, caso seja necessário. Contudo, é necessário garantir que a contratada atenda ao previsto na legislação de proteção de dados brasileira, pois ela atuará como operadora da entidade que solicitar o serviço. Assim, recomenda-se que essas empresas possam ser auditadas e que elas adotem as melhores práticas de segurança de dados disponíveis para a modalidade de eliminação.

Ainda, as entidades devem fornecer treinamento constante para seus colaboradores sobre as formas adequadas de eliminação de dados – em especial os documentos físicos. Essas medidas também incluem a disponibilização de materiais informativos (como cartilhas informacionais), acerca da proibição de que determinados documentos sejam descartados em lixo comum, de maneira a reduzir as chances de incidentes de violação à proteção de dados pessoais, e que não seja possibilitada a reconstrução da informação.

Tais práticas também estão previstas na Política de Segurança da Informação da CNI, SESI/DN, SENAI/DN e IEL/NC, a ISC nº 01/2020, que apresenta um exemplo sobre como o descarte das informações pode ser realizado:[57]

> **11.5. Descarte de informações**
> • Informações físicas devem ser descartadas via desfragmentadora ou manualmente até que impossibilite a reconstrução da informação.
> • As mídias, como *pendrive*, HDs, CDs, fitas de *backup*, devem ser descartadas seguindo um processo de descarte e controlado via inventário de ativos.

É fato que existem diversos sistemas internos por meio dos quais os dados são gerenciados e que auxiliam na organização, armazenamento e gerenciamento das informações. Contudo, na medida do possível, tais sistemas devem ser programados para permitir o descarte das informações, sendo indispensável o mapeamento dos dados armazenados pelas entidades.

Programar os *softwares* das entidades para que ocorram exclusões automáticas de dados também auxilia no processo de eliminação dos dados. Esse tipo de solução pode ser usado quando os usuários não utilizarem um sistema por determinado período, desde que os indivíduos sejam amplamente avisados sobre essa possibilidade e tenham acesso aos termos de uso e comunicados com antecedência, por diferentes meios (*e-mails*, mensagens automáticas no sítio eletrônico), que tais medidas serão empreendidas. No SENAI, por exemplo, no sistema "Meu SENAI" os dados são excluídos caso o usuário passe mais de seis meses sem utilizá-lo.

Em casos como a contratação de terceiros prestadores de serviços tecnológicos que tratam dados pessoais de colaboradores, deve-se avaliar a necessidade de revisar os contratos firmados para garantir que os parceiros comerciais também estejam em conformidade com a LGPD e adotem boas práticas de armazenamento e exclusão dos dados no período adequado.

57 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Instrução de serviço conjunta nº 01/2020**. Institui a nova política de segurança da informação no âmbito da CNI, do SESI/DN, do SENAI/DN e IEL/NC. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/f3/9c/f39c1802-591b-4254-88be-f45f6e7afd69/politica_de_seguranca_da_informacao.pdf. Acesso em: 22 jun. 2023.

3 PROTOCOLO PARA AVALIAÇÃO DE RISCO

3.1 INTRODUÇÃO

Como forma de garantir a proteção dos titulares e o desenvolvimento das atividades econômicas, a LGPD fundamenta-se em uma abordagem com base em risco. Essa abordagem requer que as operações de tratamento e a utilização de recursos tecnológicos sejam avaliados de forma casuística, devendo ser avaliada a probabilidade e extensão dos riscos das operações de tratamento. Não à toa, a ANPD incluiu na fase 1 de sua agenda regulatória[58] o debate sobre o tratamento de dados de alto risco.

Enquanto medida preventiva, a avaliação de risco é um processo voltado à gestão das atividades que se dá a partir da identificação, avaliação e monitoramento de projetos e atividades específicas. A partir desse estudo, é que serão definidos os níveis seguros de medidas técnicas e organizacionais, para que os riscos possam ser minimizados.

A Avaliação de Risco é destinada a identificar as possíveis lacunas de segurança existentes e pode auxiliar os participantes do Sistema Indústria a identificar os pontos sensíveis de melhoria em segurança, contribuindo com o direcionamento dos investimentos mais assertivos, seja financeiro, tecnológico e humano.

Por isso, é essencial que sejam mapeados todos os processos existentes nas organizações, uma vez que, por meio desse trabalho, serão identificadas as características específicas de cada entidade ou órgãos, os dados pessoais envolvidos no tratamento, qual o seu fluxo de vida, como ocorreu o compartilhamento, entre outras providências.

58 BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 11, de 27 de janeiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 22 jun. 2023.

3.2 IDENTIFICAÇÃO DE RISCOS

Com a identificação dos riscos, é necessário que se definam as chances de ocorrência (probabilidade) e prevejam os possíveis impactos caso se tornem reais. Ambos os requisitos, probabilidade e gravidade, são trazidos pela LGPD em seu art. 50, §1º.[59]

Ainda que não exista um posicionamento final da Autoridade sobre a realização da Avaliação do Risco, extrai-se da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, os seguintes critérios para definição de operações de tratamento de alto risco:

DADOS PESSOAIS DE ALTO RISCO

- **Critério geral:** tratamento de dados pessoais em larga escala ou que possa afetar significativamente interesses e direitos fundamentais dos titulares.
- **Critérios específicos:**
  - uso de tecnologias emergentes ou inovadoras;
  - vigilância ou controle de zonas acessíveis ao público;
  - decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
  - utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

Assim, o tópico seguinte destina-se a tratar de um importante instrumento relativo à avaliação de risco, exigidos pela LGPD: o Relatório de Impacto.

3.3 MODELO DE RELATÓRIO DE IMPACTO

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é um documento elaborado pelo controlador que possui a descrição dos processos de tratamento de dados pessoais capazes de gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (art. 5º, XVII, da LGPD).

59 Art. 50. *Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais*, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, *as normas de segurança*, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
§1º. Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e *a probabilidade e a gravidade dos riscos* e dos benefícios decorrentes de tratamento de dados do titular (grifo nosso).

Mesmo que até o momento não esteja claro quando e como o Relatório deve ser apresentado para a ANPD,[60] a elaboração de um RIPD é vista como uma boa prática, possibilitando o efetivo *compliance* de dados. Isso porque o RIPD tem o objetivo de avaliar, mensurar e mitigar os riscos aos titulares em tratamento de alto risco, o que significa que o titular do dado pessoal deve ser o foco do documento.

Dessa forma, ainda que as hipóteses nas quais o relatório de impacto deve ser elaborado e apresentado para a ANPD – como no caso da utilização da base legal do legítimo interesse (art. 10, §3º, da LGPD) – não tenham sido definidas pela autoridade, a elaboração do RIPD é uma boa prática e serve como um importante mecanismo de prevenção. Isso porque este instrumento busca prever os riscos, e não apenas mitigá-los após a sua ocorrência.

Tal característica pode ser extraída da decisão do STF que, ao julgar a ADI 6.387/DF, identificou o risco de a Fundação IBGE divulgar o documento apenas após o compartilhamento, já que ele "deve ser anterior à coleta e uso dos dados, e não posterior, a fim de garantir a transparência pública e medir os riscos do compartilhamento."[61] Por isso, é recomendável que este documento seja elaborado sempre antes do início de qualquer procedimento que exija o tratamento de dados pessoais de alto risco.

Nos termos do parágrafo único do art. 38 da LGPD, o relatório de impacto deve conter, no mínimo, "descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados".

Novamente, tendo em vista a necessidade de realização de análise periódica sobre a finalidade do tratamento dos dados, é indicado que sejam avaliados os riscos de toda atividade ou processo novos. Com isso, será averiguada a necessidade de produção do RIPD e se garante que a tabela de risco se mantenha atualizada, diante do caráter proativo e preliminar exigido pelo documento para proteção dos direitos dos titulares.

Assim, o RIPD auxilia o processo de decisão sobre a manutenção de atividades de alto risco, contribuindo com a eficiência e gestão dos processos de maneira mais ágil e segura. Países como Espanha e Reino Unido possuem recomendações emitidas por suas Autoridades Nacionais de Proteção de Dados.

60 A ANPD publicou uma nova tomada de subsídios sobre o tratamento de dados pessoais de alto risco. BRASIL. Participa +Brasil. **Pesquisa sobre larga escala e tratamento de alto risco ao titular de dados pessoais**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/aberta-consulta-publica-sobre-tratamento-de-dados-pessoais-de-alto-risco/GovernoFederalParticipaBrasilPesquisasobrelargaescalaetratamentodealtoriscoaotitulardedadospessoais.pdf. Acesso em: 26 set. 2022.

61 Trecho do voto do Ministro Luiz Fux. ADI 6.387/DF.

No caso espanhol,[62] o modelo publicizado inclui a necessidade de descrição do tratamento (com referência a categoria de dados afetados e responsáveis pelo tratamento), a base legal utilizada, a identificação do risco em cada uma das fases do tratamento (desde a coleta até a eliminação), bem como a análise da necessidade, alternativas e razões de escolha ao tratamento e medidas para redução de riscos e sua otimização, por exemplo.

No Reino Unido, alguns dados pessoais exigem, de pronto, a confecção de Relatório quando o tratamento de dados envolver o uso de Inteligência Artificial em tecnologias inovadoras, produção de perfilamento de um grupo de pessoas, tratamento de dados biométricos e genéticos, além de:[63]

- utilizar tecnologia inovadora (em combinação com qualquer um dos critérios das diretrizes europeias);
- utilizar perfis ou dados de categoria especial para decidir sobre o acesso aos serviços;
- traçar o perfil de indivíduos em larga escala;
- processar dados biométricos (em combinação com qualquer um dos critérios das diretrizes europeias);
- processar dados genéticos (em combinação com qualquer um dos critérios das diretrizes europeias);
- combinar dados ou combinar conjuntos de dados de diferentes fontes;
- coletar dados pessoais de uma fonte que não seja o indivíduo sem lhes fornecer um aviso de privacidade ("processamento invisível") (em combinação com qualquer um dos critérios das diretrizes europeias);
- rastrear a localização ou comportamento do indivíduo (em combinação com qualquer um dos critérios das diretrizes europeias);
- traçar o perfil das crianças ou o *marketing* ou os serviços *on-line* a elas destinados; ou
- processar dados que possam colocar em risco a saúde física ou a segurança do indivíduo no caso de uma quebra de segurança.

A definição da metodologia para a elaboração do RIPD, portanto, tem valor para a organização das atividades, promoção de previsibilidade e segurança aos titulares de dados e atores do Sistema Indústria, os quais poderão endereçar em tempo hábil as demandas que possam surgir. Logo, é importante que cada integrante tenha definido o fluxo de informações em seu âmbito, com previsões de mecanismos e protocolos a serem seguidos quando da criação de projetos ou aperfeiçoamento de processos já existentes.

62 AEPD. **La AEPD publica un modelo de informe para ayudar a las empresas a realizar evaluaciones impacto en la protección de datos**. Maio 2020. Disponível em: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-un-modelo-de-informe-para-ayudar-las-empresas. Acesso em: 26 set. 2022.

63 INFORMATION COMISSIONER'S OFFICE – ICO. **Data protection impact assessments**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. Acesso em: 26 set. 2022.

Como etapas a serem observadas para a elaboração do RIPD, é possível destacar as seguintes:[64]

ETAPAS – RELATÓRIO DE IMPACTO

1) Identificar os agentes de tratamento e o encarregado.
2) Identificar a necessidade de elaborar o Relatório de Impacto de Proteção de Dados.
3) Descrição do tratamento.
4) Identificar as partes interessadas consultadas.
5) Avaliação da necessidade e proporcionalidade.
6) Medidas previstas para demonstrar a conformidade.
7) Avaliação dos riscos para direitos e liberdades.
8) Medidas previstas para mitigar riscos.
9) Documentação.
10) Controle, com aprovação do Relatório, e reexame, com manutenção da revisão.

De acordo com as etapas anteriormente indicadas, o documento deve conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (art. 38 da LGPD).

Como a ANPD, ainda, não estabeleceu a metodologia de elaboração de RIPD,[65] sugere-se que a metodologia de elaboração do relatório seja associada à perspectiva de risco, nos termos da orientação do Relatório do *Article 29 Data Protection Working Party*[66] e outros Códigos de Boas Práticas setoriais publicados.[67]

Dessas recomendações, destacamos os seguintes aspectos fundamentais para a avaliação de risco: i) compreensão sobre as atividades desempenhadas e tipos de dados pessoais tratados; ii) identificação dos direitos dos titulares; iii) riscos envolvidos nas operações e medidas adotadas para mitigá-los; e iv) avaliação do DPO acerca dos riscos e das estratégias adotadas.

64 Adaptação do esquema apresentado pelo Relatório do Article 29 Data Protection Working Party. WP29. EUROPEAN COMMISSION. **Guidelines on Data Protection Impact Assessment (DPIA)**. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. fl 19. Acesso em: 22 jun. 2023. Esquema também disponível em: CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

65 Nesse sentido, ver: Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 28 jun. 2023.

66 Relatório do Article 29 Data Protection Working Party. WP29. EUROPEAN COMMISSION. **Guidelines on Data Protection Impact Assessment (DPIA)**. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. fl 19. Acesso em: 22 jun. 2023.

67 CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

INFORMAÇÕES DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS[68]

Descrição da atividade e dos dados pessoais	Qual a finalidade do tratamento de dados?
	Quem são os titulares dos dados?
	Qual a relação do controlador com o titular?
	Quais dados são utilizados no tratamento?
	São tratados dados sensíveis?
	O titular possui informações sobre o tratamento de dados?
	Os dados pessoais são compartilhados com terceiros?
	Os dados foram coletados diretamente dos titulares?
	O tratamento de dados é realizado com base em bases enriquecidas?
Direito dos titulares	O titular possui informações sobre o tratamento de dados?
	Os titulares possuem acesso ao relatório de dados tratados?
	Os dados são tratados por meio de decisões automatizadas?
	O tratamento de dados pode levar a tratamento discriminatório?
Riscos e mitigação	Existem riscos que podem afetar a qualidade ou confidencialidade dos dados? Se sim, quais?
	Identificar a fonte do risco.
	Quais são os eventos potencialmente lesivos?
	Existem controles, salvaguardas ou planos de ação capazes de mitigar os riscos?
	Qual a avaliação da gravidade do risco?
Avaliação DPO	Avaliação de proporcionalidade e necessidade.
	Avaliação sobre existência de atendimento aos direitos do titular.
	Avaliação sobre a estratégia de mitigação de riscos proposta.

Por fim, deve-se garantir que cada RIPD esteja adequado à situação exigida. Isto é, ao passo em que se incentiva a elaboração prévia do RIPD, em especial quando do uso da base legal do legítimo interesse, os documentos precedentes devem ser revistos e atualizados, conforme se verifique a necessidade para tal, evitando-se documentos padronizados que não atendam às solicitações e especificidades de cada tratamento.

68 A referida tabela também foi apresentada no Código de Boas Práticas do Setor de Telecomunicações. CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

4 PROTOCOLO PARA SEGURANÇA DA INFORMAÇÃO

4.1 INTRODUÇÃO

O protocolo de Segurança da Informação abrange a Segurança dos Dados Pessoais e é referenciada na LGPD por meio do princípio da Segurança (art. 6º, VII) e da Prevenção (art. 6º, VIII). Nos dispositivos da lei, é possível identificar os demais princípios correlatos à Segurança da Informação como os da integridade, autenticidade, legalidade, disponibilidade e confidencialidade. Se tais princípios forem afetados, pode-se estar diante de algum incidente de segurança da informação.

Apesar de a LGPD não definir expressamente o conceito de um incidente de segurança, as orientações da Lei, em especial no art. 46, são no sentido de que os dados devem ser resguardados por meios de medidas de segurança, técnicas e administrativas que não permitam acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Por isso, a atuação multidisciplinar quanto às medidas de Segurança da Informação é imprescindível, visto que são necessárias ações de *compliance* e integridade, tecnologia da informação, bem como contar com o apoio jurídico e de órgãos responsáveis pelo Planejamento e Gerenciamento dos Projetos Internos.

A LGPD também dispõe, no art. 48, que, caso ocorra algum incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares, o controlador tem o dever de comunicar à ANPD e ao titular. Um dos grandes desafios de se implementar um protocolo de segurança da informação, contudo, é a própria identificação de um incidente de segurança e a avaliação do risco que tal incidente pode representar para dados pessoais tratados pela organização.

O zelo com as pessoas e com os processos deve seguir acompanhado com a proteção tecnológica, evitando-se que danos sejam gerados por vulnerabilidades em *softwares* ou *hardwares* das entidades, tal qual preconiza a norma ISO 27001, o padrão e a referência Internacional para a gestão da Segurança da informação.

No âmbito das Entidades e Órgãos Nacionais do Sistema Indústria, além da observância das normas da ISO/IEC 27002:2013 (Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação); da ISO/IEC 27035:2016 (Tecnologia da informação – Técnicas de segurança – Gerenciamento de incidentes de segurança da informação); e da ITIL® v4 (*Information Technology Infrastructure Library*) – ou outras disposições que venham a substituí-las, também há normativo interno, como a ISC nº 01/2020, que disciplina a Política de Segurança da Informação em seu âmbito.

A Política de Segurança da Informação, no âmbito da CNI, do SESI/DN, do SENAI/DN e do IEL/NC, ISC nº 01/2020, mostra a maturidade deste ramo e alcança, independentemente do nível hierárquico ou tempo de vínculo, todos os colaboradores, dirigentes, terceiros, prestadores de serviços, parceiros e visitantes, no âmbito das entidades e dos órgãos nacionais.[69]

Nesse sentido, a adoção de medidas preventivas, seguida da identificação das situações em que os incidentes podem gerar riscos ou danos relevantes ao titular para, então, providências sejam tomadas em tempo hábil e o plano de ação à comunicação são etapas a serem observadas nos níveis regionais e nacionais do Sistema Indústria.

4.2 ASPECTOS PREVENTIVOS

Outros Códigos de Boas Práticas[70] vêm dispondo, de ao menos, três níveis de requisitos para prevenção dos incidentes: (i) requisitos mínimos, prévios e básicos para as atividades desenvolvidas; (ii) requisitos prioritários, que devem ser iniciados imediatamente caso ainda não tenham sido desenvolvidos plenamente na instituição; (iii) requisitos avançados, etapa posterior ao segundo nível de implementação, conforme expostos a seguir:

69 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **ISC nº 01/2020**. Institui nova Política de Segurança da Informação no âmbito da CNI, do SESI/DN, do SENAI/DN e do IEL/NC. P. 7. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/f3/9c/f39c1802-591b-4254-88be-f45f6e7afd69/politica_de_seguranca_da_informacao.pdf. Acesso em: 22 jun. 2023.

70 Exemplos são o Código de Boas Práticas editado pela CNSaúde e o Conexis. CNSAÚDE. **Código de Boas Práticas de proteção de dados para os prestadores privados em saúde**. 2021. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 22 jun. 2023. Código de boas práticas de proteção de dados para o setor de telecomunicações. CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

REQUISITOS DE SEGURANÇA MÍNIMOS	
Políticas e Conscientização	Criar, revisar e comunicar diretrizes considerando melhores práticas para assegurar a proteção e privacidade dos dados pessoais.
Gestão de Identidades e Acessos	Fornecer acessos somente às pessoas autorizadas e revogá-los quando não forem mais necessários ou a pessoa não trabalhar mais na empresa.
Gestão de *Backups*	Garantir que os dados relevantes para o negócio tenham uma cópia de segurança, devidamente protegida contra acessos não autorizados.
Gestão de Ativos	Inventariar os ativos que tratam dados pessoais e garantir os requisitos mínimos de segurança.
Gestão de Segurança *Endpoint*	Garantir que todos os ativos que tratam dados pessoais tenham uma solução de *antimalware* e *personal firewall* instalada e atualizada periodicamente.

REQUISITOS DE SEGURANÇA PRIORITÁRIOS	
Monitoramento e Gestão de Incidentes	Monitorar o comportamento dos acessos e da segurança dos ativos envolvidos no tratamento dos dados. Esteja preparado para identificar comportamentos e/ou acessos não autorizados.
Gestão de Fornecedores	Avaliar se o fornecedor contratado possui cláusulas contratuais de segurança e privacidade quanto ao tratamento de dados pessoais.
***Log* de sistemas críticos**	Avaliar e garantir que sejam registradas as atividades de tratamentos dos dados: data, horário, duração, identidade do funcionário/responsável pelo acesso e a ação executada/processada.
Controle para Vazamento de Informações	Prevenir o vazamento dos dados pessoais em todo o seu ciclo de tratamento.
Segurança Física	Garantir a segurança do acesso físico às informações tratadas em mídias eletrônicas, papel e sistemas.
Gestão de Vulnerabilidade / *Pentest*	Avaliar a execução de testes de segurança nos sistemas que tratam dados pessoais, priorizando os sistemas expostos na internet.
Transferência de Dados	Garantir a segurança na comunicação durante os processos de transferências de dados.

REQUISITOS DE SEGURANÇA AVANÇADOS	
Arquitetura de Segurança	Analisar e identificar melhorias para a proteção dos dados pessoais envolvendo a arquitetura de tecnologias que suportam os produtos/sistemas, incluindo *Cloud*.
Exclusão de Dados Tratados	Mapear a localização dos dados pessoais para que possam ser excluídos quando solicitado.
Mascaramento de Dados	Avaliar o uso de mascaramento de dados quando aplicável.
Pseudoanonimização	Avaliar o uso de pseudonimização quando aplicável.
Desenvolvimento Seguro	Avaliar se o produto ou sistema estão integrados na esteira atual que contempla análise e implementação de requisitos de segurança para o desenvolvimento seguro.
Criptografia	Avaliar a utilização de recursos de criptografia de dados pessoais quando necessária.

O primeiro nível de segurança envolve ações como a já mencionada criação de políticas e conscientização com os colaboradores, promovendo diretrizes a exemplo do Guia de Boas Práticas. Entre as iniciativas voltadas especificamente para os colaboradores, podemos citar:

Iniciativas para conscientização de colaboradores sobre segurança da informação:

- Realização de treinamentos periódicos de acordo com as atribuições e responsabilidades de cada colaborador na instituição, além de um treinamento específico no momento da contratação.
- O treinamento deve apresentar boas práticas e incluir medidas básicas de segurança, abordando conceitos como privacidade e proteção de dados pessoais, escolha de senhas fortes para utilização de serviços *on-line*, adoção de medidas como autenticação multifator e instalação de programas antivírus em equipamentos pessoais que possam ter conexão com a rede profissional.
- Utilização de diferentes formatos de treinamento, como *workshops*, estudos de casos reais da empresa e estudos de casos práticos de outras empresas ou da própria instituição.
- Utilização de mecanismos diversos de compartilhamento de informações sobre proteção de dados, como, por exemplo, anúncios nos *sites* da instituição ou boletins informativos.
- Disponibilização de materiais para consulta contínua, como gravações de vídeos e materiais instrutivos *on-line* ou impressos.
- Monitoramento da execução das instruções fornecidas, incluindo métricas relevantes, como o número de pessoas treinadas e os períodos de treinamento.
- Instrução dos funcionários responsáveis pelo atendimento ao para que tenham cuidado com os meios utilizados (*e-mail* ou telefone) e informações compartilhadas, além de terem clareza sobre quais informações não são autorizadas, ou podem ser consideradas confidenciais ou sensíveis.
- Instrução dos funcionários a identificar atividades suspeitas e reportá-las imediatamente aos setores responsáveis. Tais atividades suspeitas podem incluir o surgimento de *pop-ups* estranhos, lentidão no dispositivo ou perda de controle do mouse ou teclado.
- Estabelecimento de mecanismos de controle de remetentes e conteúdos de *e-mails* quando não for possível garantir sua segurança e veracidade.

A segunda etapa, de requisitos de segurança prioritários, refere-se a ações como o monitoramento do comportamento dos acessos de segurança dos ativos que tratam dados e gestão de incidentes, para que acessos ou comportamentos não autorizados sejam identificados, bem como prevenir que se tenha vazamento de informações em todo o ciclo de tratamento de dados.

Sobre a terceira etapa, os requisitos de segurança avançados envolvem a construção de uma arquitetura de segurança, aplicável aos sistemas e produtos utilizados pelas instituições. Envolvem, além disso, a adoção de técnicas – como o mascaramento de dados –, a pseudonimização, criptografia, mapeamento do fluxo de dados internos e procedimentos de sua exclusão quando solicitados pelos titulares ou se tenha o término do tratamento.

A Política de Segurança da Informação da CNI, SESI/DN, SENAI/DN e IEL/DN – ISC nº 01/2020[71] – apresenta um exemplo de diretrizes valiosas sobre segurança da informação sob a perspectiva preventiva. Destacamos a distribuição de diferentes responsabilidades para os atores envolvidos no ecossistema de dados do Sistema Indústria (item 6. Responsabilidades):

Colaboradores, dirigentes, terceiros e prestadores de serviços (6.1.)

- Compreender e cumprir a Política de Segurança de Informação.
- Obedecer à devida classificação das informações.
- Estar de acordo com os termos de responsabilidade e confidencialidade.
- Comunicar possíveis desvios de conduta quanto à Política por meio do canal de reporte a incidentes de segurança.
- Fazer bom uso das informações.
- Ser agente de segurança dentro e fora da organização, apoiando as demais Federações e Departamentos Regionais (DRs), sempre que necessário.
- Reportar qualquer desvio identificado para o responsável imediato.

Presidência (6.2.)

- Direcionar as ações estratégicas de Segurança da Informação.

Comitê de Segurança da Informação e proteção de dados (6.3)

- Fomentar o assunto Segurança da Informação e Proteção de Dados em toda estrutura organizacional.
- Debater, definir e aprimorar os controles estabelecidos na PSI.
- Apoiar as diretorias e os gestores na tratativa de incidentes de segurança.
- Estruturar os programas de comunicação focados em conscientização dos colaboradores, dirigentes, terceiros, prestadores de serviço e parceiros e visitantes, no tema Segurança da Informação e Proteção de Dados.

Diretoria, Superintendência e Gerências (6.4)

- Apoiar a divulgação do tema e promover a conscientização dos colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros e visitantes, quanto à aderência das práticas às ações de segurança.
- Fiscalizar e certificar colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros e visitantes, quanto à aderência das práticas às ações de segurança.

Parceiros e visitantes (6.5)

- Seguir as políticas e os normativos de segurança estabelecidos.

Também se chama atenção para a classificação e manuseio das informações apresentadas pela política, que pode ser utilizada como exemplo de boas práticas para outras instituições. Entre as informações tratadas pelo Sistema Indústria, destaca-se a necessidade de adoção de cuidados adicionais em relação aos seguintes dados:[72]

71 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA –CNI. **Instrução de Serviço conjunta nº 01/2020**. Política de Segurança da Informação das entidades e órgãos nacionais do Sistema Indústria. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/f3/9c/f39c1802-591b-4254-88be-f45f6e7afd69/politica_de_seguranca_da_informacao.pdf. Acesso em: 22 jun. 2023.

72 Tipologia apresentada na Minuta da Norma de Gerenciamento de Incidentes de Segurança elaborada pelo Comitê de Segurança da Informação e Comitê Técnico de LGPD e pelo Grupo Técnico composto pela STI – Superintendência de Tecnologia da Informação; Sucom – Superintendência de *Compliance* e Integridade; DJ – Diretoria Jurídica; Geplano – Gerência de Planejamento, Projetos e Processos.

a) **Dados financeiros:** em razão do vazamento de dados financeiros elevar, consideravelmente, o risco do incidente de segurança considerando o potencial dano que o titular dos dados possa sofrer.
b) **Dados relacionados a *logins* e senhas:** em razão destes dados pessoais viabilizarem o acesso a informações confidenciais do titular.
c) **Dados de geolocalização**: em razão de o vazamento permitir que criminosos ou terceiros acompanhem os deslocamentos do titular, aumentando significativamente o risco do incidente de segurança, uma vez que podem fornecer informações que viabilizem a prática de crimes como roubos e sequestros.

Entre esses cuidados, pode-se mencionar como exemplo a criação de restrição de acesso por meio do controle de acesso (item 11.6 da ISC nº 01/2020), classificação das informações em níveis mais elevados de confidencialidade quando elas envolverem esses tipos de dados (item 11.3 da ISC nº 01/2020), além de controle das áreas seguras considerando a existência desses dados nas instalações das entidades (item 11.9 da ISC nº 01/2020).

Quanto aos dados no meio físico, práticas como anotar o *login* e a senha em *post-it* e colá-los na área de trabalho, usar as mesmas senhas para diferentes sistemas, por exemplo, devem ser evitados, além do armazenamento de documentos ocorrer em gavetas ou armários com chave e desligamento dos equipamentos ao fim do expediente. Outras medidas podem ser desenvolvidas em parceria com os colaboradores do Sistema Indústria, seguindo o exemplo da Política de Mesa e tela limpa (item 11.12 – ISC nº 01/2020).

Do mesmo modo, os colaboradores devem seguir as orientações da "Norma – Política de Senhas", desenvolvida e disponível internamente ao Sistema Indústria:

11.2. Política mesa e tela limpa:

- As informações quando físicas (impressas) ou até mesmo em formato digital, devem ser posicionadas de maneira organizada para mitigar a possibilidade de acesso indevido.
- Sempre que possível as informações físicas devem ser armazenadas em gavetas ou armários com chave.
- A classificação da informação deve ser considerada para que o tratamento seja adequado.

É dever de todos os colaboradores, dirigentes, terceiros, prestadores de serviço:

- Garantir que, fora do expediente de trabalho, os documentos impressos, mídias eletrônicas e demais objetos sejam guardados em locais apropriados, como armários, cofres ou qualquer tipo de mobília que possua chave.
- Desligar todas as estações de trabalho no fim do expediente.
- Descartar os *flip charts* usados e apagar todas as informações da lousa, após o uso das salas.
- Bloquear a tela, sempre que se ausentar da estação de trabalho.
- Evitar a impressão de documentos sensíveis, sempre que possível.

Adicionalmente, é importante que se preze pelo desenvolvimento seguro de produtos e sistemas, abrangendo aspectos, como a gestão de vulnerabilidade e transferência de dados, de forma a assegurar a análise e implementação de requisitos de segurança para o desenvolvimento confiável.

4.3 IDENTIFICAÇÃO DE INCIDENTE DE SEGURANÇA E ANÁLISE DE RISCO

A LGPD prevê a centralidade dos agentes de tratamento de dados na adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de incidentes de segurança (art. 46). Os controladores e operadores, no âmbito de suas competências, podem formular regras de boas práticas de governança para o tratamento de dados pessoais, contando inclusive com um programa de governança em privacidade que conte com planos de resposta a incidentes e remediação (art. 50, §2°, I).

Entre as condutas que podem provocar incidentes de segurança da informação, é possível indicar casos em que arquivos físicos, como documentos administrativos, sejam indevidamente descartados por algum colaborador enquanto ainda estavam sendo utilizados, representando uma situação acidental ou ilícita de destruição.

Percebe-se que os casos de incidente de segurança não se limitam a ataques *hackers*, com invasão dos sistemas tecnológicos, mesmo que a divulgação de dados na internet seja extremamente grave a depender do volume e grau de informações disponíveis. Na verdade, o fator humano é uma grande vulnerabilidade, uma vez que as pessoas podem ser mais suscetíveis a erros, intencionais ou não. Isso reforça o cuidado que as entidades do Sistema Indústria devem ter com treinamento e capacitações habituais com seus colaboradores, além de políticas, como a "mesa limpa", anteriormente destacadas.

Aliado a essa percepção, o constante monitoramento e a revisão das atividades, mencionadas anteriormente para garantir o cumprimento das finalidades do tratamento dos dados, é relevante para identificar procedimentos ineficazes que possam comprometer a segurança das informações. Assim, não apenas os dados dos titulares são resguardados, como também o próprio patrimônio das organizações.

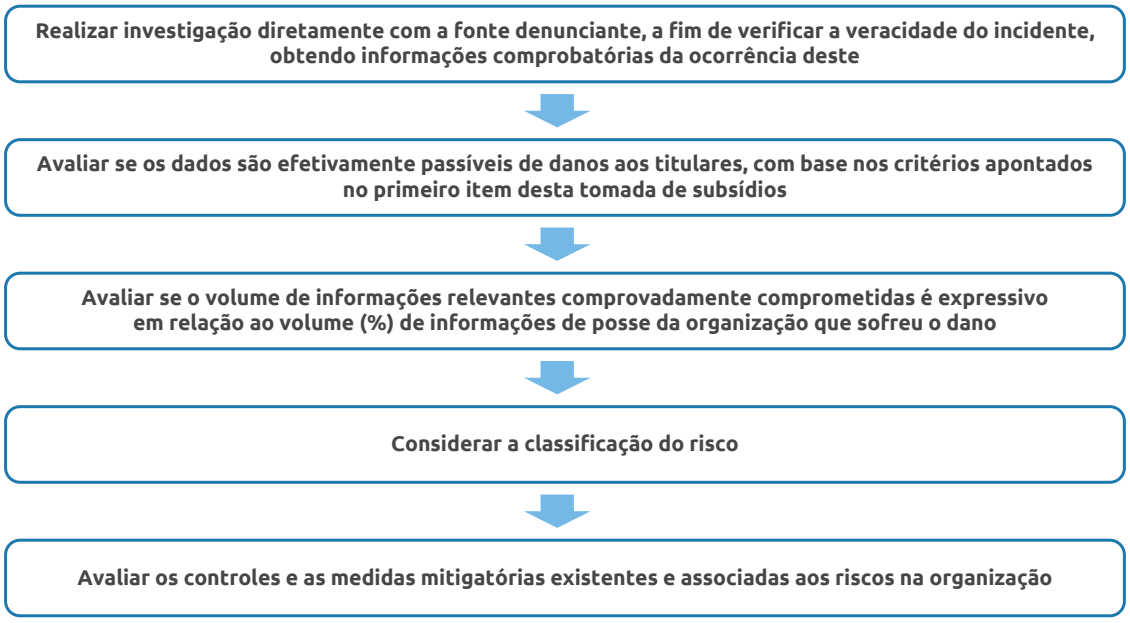
Sob tal perspectiva, a identificação de incidentes deve ser aprimorada com todos os colaboradores, para que eles sejam capazes de observar possíveis falhas e comunicar assim que possível aos responsáveis para que as medidas legais sejam tomadas. Esse processo, contudo, não é uma atividade simples.

A identificação de um incidente de segurança exige a descoberta de um possível incidente, seguido da averiguação capaz de comprovar ou não se o incidente ocorreu, o que deve ser providenciado no menor tempo possível. Após a confirmação do risco ou danos aos titulares, passa-se às etapas de comunicações externas, isto é, à ANPD e aos titulares, caso aplicável, em tempo razoável. Por fim, recomenda-se a elaboração de documento com o registro de todas as ações tomadas e providências voltadas à melhoria, de forma que o RIPD possa ser atualizado.

A avaliação de risco ou de dano relevante pode ser feita por meio de métricas e parâmetros aplicados no contexto brasileiro. Assim, o controlador deve considerar uma combinação da gravidade do impacto potencial (I) sobre os direitos e liberdades dos indivíduos e a probabilidade da sua ocorrência (P).[73]

Nesta análise, os aspectos da volumetria, tipologia e exposição são pertinentes a serem verificados. A volumetria refere-se à quantidade de registros afetados no incidente; enquanto a tipologia está relacionada à categoria do dado, se pessoal ou se pessoal sensível. A exposição é correlata ao ambiente em que o incidente foi exposto, que pode ter maior gravidade se varia de interno, externo e público.[74]

Da mesma forma, é incentivado que o máximo de evidências que ocorreram a partir da ciência do incidente sejam preservadas, com toda a rede de diligências, providências e mitigação dos riscos. Isto se justifica para o caso de eventualmente demais autoridades públicas solicitarem informações sobre os fatos posteriormente, por exemplo.[75]



73 CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

74 CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

75 CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

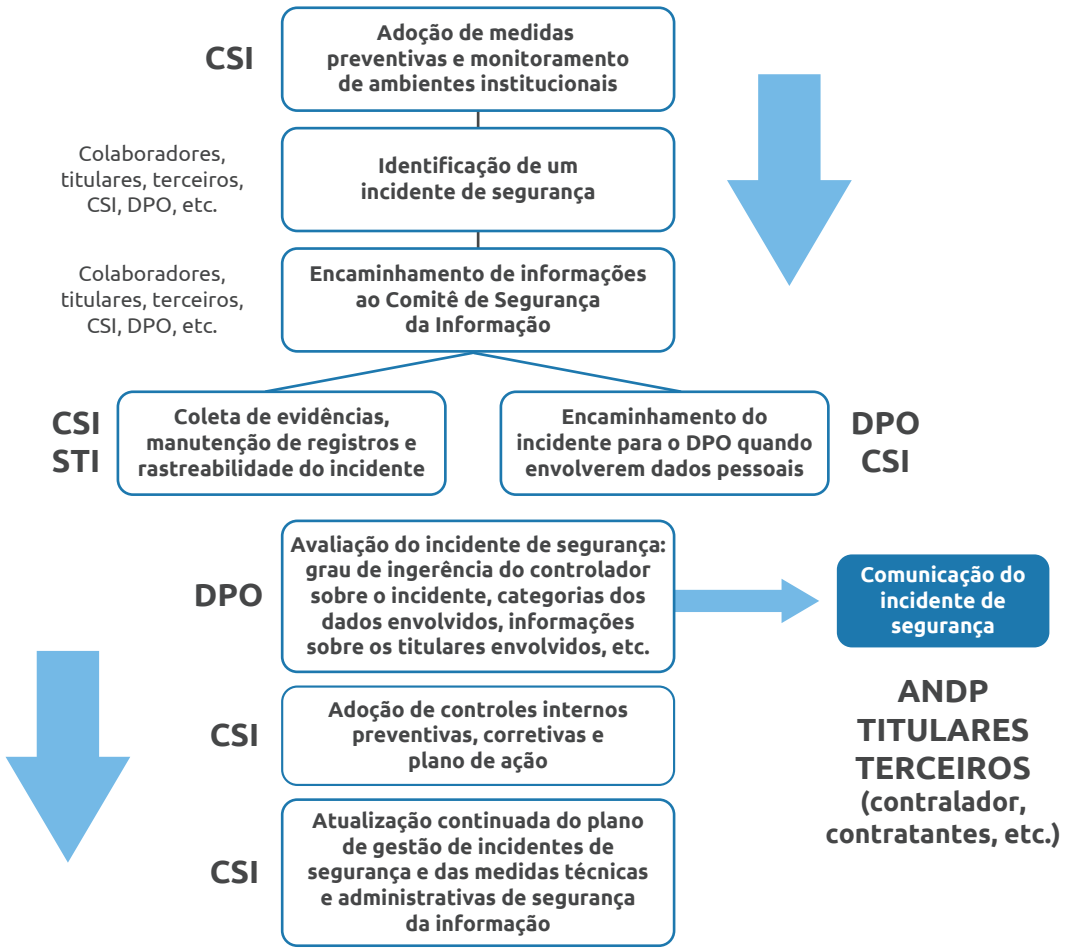
***CHECKLIST* – AVALIAÇÃO DO INCIDENTE DE SEGURANÇA**

- ☑ **Natureza, sensibilidade e volume de dados pessoais:**
  – Perda de integralidade de dados.
  – Indisponibilidade de dados.
- ☑ **Veracidade do incidente.**
- ☑ **Facilidade da identificação dos titulares:**
  – Dados anonimizados e/ou criptografados.
  – Titulares relacionados às chaves de criptografia dos dados violados.
  – Dados relacionados às credenciais de autenticação (matrícula, por exemplo) das partes interessadas.
- ☑ **Nível de atualização e validade dos dados.**
- ☑ **Severidade das consequências aos titulares.**
- ☑ **Características especiais dos titulares.**
- ☑ **Número de titulares afetados.**
- ☑ **Grau de exposição de dados vulnerados** (ambiente interno, externo e público).
- ☑ **Medidas técnicas, organizacionais e administrativas adotadas para mitigar o impacto sobre os titulares.**
- ☑ **Aspectos relacionados à violação de segurança para acesso aos dados** (intencional, não intencional, ataque cibernético).
- ☑ **Se o responsável pelo dado objeto do incidente auferiu, direta ou indiretamente, vantagem com o ocorrido.**
- ☑ **Se o ambiente afetado pelos incidentes está relacionado ao país de operação de negócio do controlador/operador.**

4.4 FLUXO INTERNO DE COMUNICAÇÃO DE POSSÍVEL INCIDENTE DE SEGURANÇA

O fluxo interno de comunicação, nas hipóteses de incidente de segurança, deve facilitar a comunicação eficiente e rápida para que qualquer colaborador que identificar a ocorrência de um incidente possa direcionar ao setor responsável. Entre os agentes envolvidos, como exemplo, no âmbito das entidades e órgãos nacionais do Sistema Indústria, podemos mencionar: i) Comitê de Segurança da Informação e de Proteção e Dados (CSI); ii) Diretoria Jurídica (DPO); iii) Superintendência de Tecnologia da Informação (STI); iv) colaboradores; v) titulares; vi) terceiros.

Com base na estrutura anterior, grosso modo, a comunicação dos incidentes de segurança devem ser feitos da seguinte forma:[76]



Veja-se que o encarregado deve providenciar investigação sobre o incidente, verificando a sua ocorrência. No canal, é aconselhável que se tenha um Formulário de Comunicação Interna de Incidente de Segurança, o qual possa abranger, por exemplo:

- Tipo do incidente de segurança (ação maliciosa, erro humano ou falhas nos sistemas).
- Origem da identificação/alerta.
- Sistemas e ou ativos afetados.
- Área e unidade em que ocorreu o incidente.
- Data e hora da identificação do incidente.
- Classificação da gravidade do incidente: entre baixa, média, alta e muito alta.
- Possíveis impactos aos pilares de segurança da informação.

76 Representação visual do fluxo descrito na Política de Segurança da Informação da CNI, SESI/DN, SENAI/DN e IEL/DN – ISC nº 01/2020 e na Minuta da Norma de Gerenciamento de Incidentes de Segurança elaborada pelo Comitê de Segurança da Informação e Comitê Técnico de LGPD e pelo Grupo Técnico composto pela STI –Superintendência de Tecnologia da Informação; Sucom – Superintendência de *Compliance* e Integridade; DJ – Diretoria Jurídica; Geplano – Gerência de Planejamento, Projetos e Processos.

- Possíveis impactos aos titulares dos dados.
- Descrição do incidente, com a inserção de outras informações julgadas pertinentes como o detalhamento da causa.
- Evidências, como *Printscreen*.

As entidades e órgãos devem cooperar entre si para que, em atenção ao fluxo de dados existente, o contato entre os encarregados, controladores e operadores seja facilitado e incentivado, em especial com as áreas de *Compliance* e Tecnologia da Informação.

Novamente, a promoção de uma cultura de proteção de dados é incentivada para que se evite a divulgação, com intenção ou não, dos incidentes de forma inapropriada pelos colaboradores.

4.5 COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

A ANPD recomenda[77] que nos casos em que se constatarem incidentes de segurança, deve-se:

i) Avaliar internamente o incidente – natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis;

ii) Comunicar ao encarregado (art. 5º, VIII da LGPD).

iii) Comunicar ao controlador, se for o operador, nos termos da LGPD.

iv) Comunicar à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares (art. 48 da LGPD).

v) Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (art. 6º, X, da LGPD).

Ainda que existam dúvidas sobre a extensão e gravidade dos danos, é relevante que os controladores adotem posição de cautela, para que mesmo nestes casos a comunicação seja realizada. Excepcionalmente, é possível que a ANPD analise as informações prestadas pelo operador.

Em todas as hipóteses, a comunicação deve ser clara e precisa, podendo ser complementada posteriormente quando não for possível indicar a integralidade das informações.

77 BRASIL. Autoridade Nacional de Proteção de Dados. **Comunicação de incidentes de segurança**. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 22 jun. 2023.

Na ocorrência de um incidente de segurança a ANPD recomenda a comunicação das seguintes informações:[78]

Identificação e dados de contato de:

- Entidade ou pessoa responsável pelo tratamento.
- Encarregado de dados ou outra pessoa de contato.
- Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.

Informações sobre o incidente de segurança com dados pessoais:

- Data e hora da detecção.
- Data e hora do incidente e sua duração.
- Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, entre outros.
- Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados.
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento.
- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados.
- Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD.
- Resumo das medidas implementadas até o momento para controlar os possíveis danos.
- Possíveis problemas de natureza transfronteiriça.
- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Ademais, a Autoridade também solicita que o seguinte formulário seja preenchido, como forma de facilitar o processo de comunicação de incidentes pelos controladores de dados pessoais:[79]

78 Para mais informações acessar: BRASIL. Autoridade Nacional de Proteção de Dados. **Comunicação de incidentes de segurança**. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 22 jun. 2023.

79 Reproduzimos o mais recente formulário disponibilizado pela ANPD. BRASIL. Autoridade Nacional de Proteção de Dados. **Coordenação-Geral de Fiscalização da ANPD divulga novo formulário para envio de Comunicados de Incidentes de Segurança.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/coordenacao-geral-de-fiscalizacao-da-anpd-divulga-novo-formulario-para-envio-de-comunicados-de-incidentes-de-seguranca. Acesso em: 23 dez. 2022. Atualmente, a ANPD indica que o formulário deve ser protocolado eletronicamente por meio do Peticionamento Eletrônico do SUPER.BR (Sistema Único de Processo Eletrônico em Rede). Diante da possibilidade de atualizações, é recomendável o acompanhamento rotineiro sobre as atividades da ANPD.

Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD)

Dados do Controlador	
Razão Social / Nome:	
CNPJ/CPF:	
Endereço:	
Cidade:	Estado:
CEP:	
Telefone:	E-mail:
Declara ser Microempresa ou Empresa de Pequeno Porte:	( ) Sim ( ) Não
Declara ser Agente de Tratamento de Pequeno Porte[80]:	( ) Sim ( ) Não
Informe o número aproximado de titulares cujos dados são tratados por sua organização:	
Dados do Encarregado	
Possui um encarregado pela proteção de dados pessoais?	( ) Sim ( ) Não
Nome:	
CNPJ/CPF:	
Telefone:	E-mail:
Dados do Notificante / Representante Legal	
( ) O próprio encarregado pela proteção de dados.	
( ) Outros (especifique):	
Nome:	
CNPJ/CPF:	
Telefone:	
E-mail:	
A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente. • *Encarregado*: ato de designação/nomeação/procuração. • *Representante*: contrato social e procuração, se cabível.	

80 Nos termos do Regulamento de Aplicação da Lei nº 13.709, de 14 de agosto de 2018, aprovado pelo BRASIL. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 jun. 2023.

Tipo de Comunicação	
( ) Completa	*Todas as informações a respeito do incidente estão disponíveis e **a comunicação aos titulares já foi realizada**.*
( ) Preliminar	*Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a **comunicação aos titulares ainda não foi realizada**.* *A complementação deverá ser encaminhada em até **30 dias corridos** da comunicação preliminar.*
( ) Complementar	*Complementação de informações prestadas em comunicação preliminar.*

A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.

- A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.

Avaliação do Risco do Incidente
( ) O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
( ) O incidente não acarretou risco ou dano relevante aos titulares. **(Comunicação Complementar)**
( ) O risco do incidente aos titulares ainda está sendo apurado. **(Comunicação Preliminar)**
Justifique, se cabível, a avaliação do risco do incidente:

Da Ciência da Ocorrência do Incidente		
Por qual meio se tomou conhecimento do incidente?		
( ) Identificado pelo próprio controlador.	( ) Notificação do operador de dados.	( ) Denúncia de titulares/ terceiros.
( ) Notícias ou redes sociais.	( ) Notificação da ANPD.	( ) Outros. (especifique)
Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:		
Caso o incidente tenha sido comunicado ao controlador por um operador, informe: **Dados do Operador** Razão Social / Nome: CNPJ/CPF: E-mail:		
Cabe ao controlador solicitar ao operador as informações necessárias à comunicação do incidente.		

Da Tempestividade da Comunicação do Incidente
Informe as seguintes datas, sobre o incidente: Quando ocorreu Quando tomou ciência Quando comunicou à ANPD Quando comunicou aos titulares
Justifique, se cabível, a não realização da comunicação completa à ANPD e aos titulares de dados afetados no prazo sugerido de 2 (dois) dias úteis após a ciência do incidente:
Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:

Da Comunicação do Incidente aos Titulares dos Dados	
Os titulares dos dados afetados foram comunicados sobre o incidente?	
( ) Sim.	( ) Não, mas o processo de comunicação está em andamento.
( ) Não, por não haver risco ou dano relevante a eles.	( ) Não, vez que o risco do incidente ainda está sendo apurado. (**comunicação preliminar**)
Se cabível, quando os titulares serão comunicados sobre o incidente?	
De que forma a ocorrência do incidente foi comunicada aos titulares?	
( ) Comunicado individual por escrito. *(mensagem eletrônica / carta / e-mail / etc.)*	( ) Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.
( ) Comunicado individual por escrito com confirmação de recebimento. *(mensagem eletrônica / carta / e-mail / etc.)*	( ) Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (*especifique abaixo*)
( ) Outros. (*especifique abaixo*)	( ) Não se aplica.
Descreva como ocorreu a comunicação:	
Quantos titulares foram comunicados individualmente sobre o incidente?	
Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:	
O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações: 1. resumo e data de ocorrência do incidente; 2. descrição dos dados pessoais afetados; 3. riscos e consequências aos titulares de dados; 4. medidas tomadas e recomendadas par mitigar seus efeitos, se cabíveis; 5. dados de contato do controlador para obtenção de informações adicionais sobre o incidente.	

O comunicado aos titulares atendeu os requisitos acima?

( ) Sim ( ) Não

- Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado.
- Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.

Descrição do Incidente

Qual o tipo de incidente? (Informe o tipo mais específico)

( ) Sequestro de Dados (*ransomware*) sem transferência de informações.	( ) Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações.
( ) Exploração de vulnerabilidade em sistemas de informação.	( ) Vírus de Computador / *Malware*.
( ) Roubo de credenciais / Engenharia Social.	( ) Violação de credencial por força bruta.
( ) Publicação não intencional de dados pessoais.	( ) Divulgação indevida de dados pessoais.
( ) Envio de dados a destinatário incorreto.	( ) Acesso não autorizado a sistemas de informação.
( ) Negação de Serviço (DoS).	( ) Alteração/exclusão não autorizada de dados.
( ) Perda/roubo de documentos ou dispositivos eletrônicos.	( ) Descarte incorreto de documentos ou dispositivos eletrônicos.
( ) Falha em equipamento (hardware).	( ) Falha em sistema de informação (*software*).
( ) Outro tipo de incidente cibernético. (especifique abaixo)	( ) Outro tipo de incidente não cibernético. (especifique abaixo)

Descreva, resumidamente, como ocorreu o incidente:

Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):

Que medidas foram adotadas para corrigir as causas do incidente?

Impactos do Incidente Sobre os Dados Pessoais

De que forma o incidente afetou os dados pessoais (admite mais de uma marcação):

( ) Confidencialidade	Houve acesso não autorizado aos dados, violando seu sigilo.
( ) Integridade	Houve alteração ou destruição de dados de maneira não autorizada ou acidental.
( ) Disponibilidade	Houve perda ou dificuldade de acesso aos dados por período significativo.

Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admite mais de uma marcação)

( ) Origem racial ou étnica. ( ) Convicção regiliosa. ( ) Opinião política.

( ) Referente à saúde. ( ) Biométrico. ( ) Genético.

( ) Referente à vida sexual. ( ) Filiação a organização sindical, religiosa, filosófica ou política.

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

Quais os demais tipos de dados pessoais violados? (admite mais de uma marcação)

( ) Dados básicos de identificação *(ex: nome, sobrenome, data de nascimento, matrícula)*

( ) Número de documentos de identificação oficial. *(ex: RG, CPF, CNH, passaporte)*

( ) Dados de contato. (*ex: telefone, endereço, e-mail*)

( ) Dados de meios de pagamento. *(ex: cartão de crédito/débito)*

( ) Cópias de documentos de identificação oficial.

( ) Dados protegidos por sigilo profissional/legal.

( ) Dado financeiro ou econômico.

( ) Nomes de usuário de sistemas de informação.

( ) Dado de autenticação de sistema. (*ex: senhas, PIN ou tokens)*

( ) Imagens / Áudio / Vídeo

( ) Dado de geolocalização. *(ex: coordenadas geográficas)*

( ) Outros (especifique abaixo)

Descreva os tipos de dados pessoais não sensíveis violados:

Riscos e Consequências aos Titulares dos Dados

Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?

( ) Sim ( ) Não

Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?

Qual a quantidade aproximada de titulares afetados[81] pelo incidente?

Total de titulares afetados

Crianças e/ou adolescentes

Outros titulares vulneráveis

Se aplicável, descreva as categorias de titulares vulneráveis afetados:

81 Titular afetado é aquele cujos dados podem ter tido a confidencialidade, a integridade ou a disponibilidade violadas e que ficará exposto a novos riscos relevantes em razão do incidente.

Quais a categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação)

( ) Funcionários.	( ) Prestadores de serviços.	( ) Estudantes/Alunos.
( ) Clientes/Cidadãos.	( ) Usuários.	( ) Inscritos/Filiados.
( ) Pacientes de serviço de saúde.	( ) Ainda não identificadas.	( ) Outros. (especifique abaixo)

Informe o quantitativo de titulares afetados, por categoria:

Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação)

( ) Danos morais.	( ) Danos materiais.	( ) Violação à integridade física.
( ) Discriminação social.	( ) Danos reputacionais.	( ) Roubo de identidade.
( ) Engenharia social / Fraudes.	( ) Limitação de acesso a um serviço.	( ) Exposição de dados protegidos por sigilo profissional/legal.
( ) Restrições de direitos.	( ) Perda de acesso a dados pessoais.	( ) Outros (especifique abaixo).

Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:

Qual o provável impacto do incidente sobre os titulares? (admite só uma marcação)

( ) Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.

( ) Podem sofrer danos, superáveis com certa dificuldade.

( ) Podem sofrer danos importantes, superáveis com muita dificuldade.

( ) Podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou tem potencial para ocasionar dano significativo ou irreversível.

Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?

Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais

Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?

( ) Sim, integralmente protegidos por criptografia / pseudonimização.	( ) Sim, parcialmente protegidos por criptografia / pseudonimização.	( ) Não.

Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:

Antes do incidente, quais das seguintes medidas de segurança eram adotadas? (admite mais de uma marcação)

( ) Políticas de segurança da informação e privacidade.	( ) Processo de Gestão de Riscos.	( ) Registro de incidentes.
( ) Controle de acesso físico.	( ) Controle de acesso lógico.	( ) Segregação de rede.
( ) Criptografia/Anonimização.	( ) Cópias de segurança. (*backups*)	( ) Gestão de ativos.
( ) Antivírus.	( ) Firewall.	( ) Atualização de Sistemas.
( ) Registros de acesso (logs).	( ) Monitoramento de uso de rede e sistemas.	( ) Múltiplos fatores de autenticação.
( ) Testes de invasão.	( ) Plano de resposta a incidentes.	( ) Outras (especifique).

Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:

Após o incidente, foi adotada alguma nova medida de segurança? (admite mais de uma marcação)

( ) Políticas de segurança da informação e privacidade.	( ) Processo de Gestão de Riscos.	( ) Registro de incidentes.
( ) Controle de acesso físico.	( ) Controle de acesso lógico.	( ) Segregação de rede.
( ) Criptografia/Anonimização.	( ) Cópias de segurança. (*backups*)	( ) Gestão de ativos.
( ) Antivírus.	( ) Firewall.	( ) Atualização de Sistemas.
( ) Registros de acesso (logs).	( ) Monitoramento de uso de rede e sistemas.	( ) Múltiplos fatores de autenticação.
( ) Testes de invasão.	( ) Plano de resposta a incidentes.	( ) Outras (especifique).

Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:

As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?

( ) Sim ( ) Não

Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.

<ASSINATURA>

4.6 PLANO DE AÇÃO APÓS A COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

Identificados a falha e os riscos gerados pelos incidentes de segurança, é apropriado que um plano de ação seja editado para que tais erros não sejam mais repetidos. Esse plano deve ser revisado de forma periódica, e as medidas utilizadas nas entidades devem ser constantemente aprimoradas para evitar que incidentes futuros ocorram.

Para tanto, as medidas técnicas e administrativas recomendadas podem se dividir no âmbito da governança e da Tecnologia da Informação (TI).[82]

Medidas administrativas no âmbito da governança

- Políticas corporativas.
- Treinamentos, capacitação de colaboradores, comunicação e aculturamento.
- Contratos: inclusão de anexos de SI e LGPD; revisão; cláusulas; DPA.
- Comitês de Crise e Executivo.
- Políticas de privacidade, de *cookies*, termos de uso para *sites* e aplicativos.
- Controles, entre outros.

Medidas técnicas adotadas no âmbito da Tecnologia da Informação

- Análise e seleção de fornecedores por meio de processo de *Vendor Assessment*.
- Utilização de ferramenta de *Data Loss Prevention* (DLP).
- Simulados de incidentes de segurança, a fim de verificar a aderência ao Plano de Gerenciamento de Incidentes.
- Realização de testes de invasão dentro do processo de desenvolvimento com o objetivo de que as aplicações sejam publicadas com a menor quantidade possível de vulnerabilidades.
- Mapeamento das superfícies de ataque interna e externa visando identificar ativos não documentados e vetores de ataques ao ambiente.
- Testes de invasão nos ativos críticos legados e/ou que não estejam integrados à esteira *DevSecOps*.
- Monitoramento contínuo dos sistemas por meio de testes recorrentes nesses sistemas/aplicações em ambiente produtivo.
- Realização de testes visando a fortalecer os mecanismos de monitoramento, detecção e resposta frente a ameaças cibernéticas.
- Processo de identificação de vulnerabilidades por meio de ferramentas automatizadas;
- Governar o processo de aplicação de *patches* por meio do monitoramento de *patches* de segurança lançados e avaliação do ambiente para aplicação destes *patches* de acordo com suas criticidades e impactos para o negócio.

82 CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

5 PROTOCOLO PARA O TRATAMENTO DE DADOS DE FUNCIONÁRIOS

5.1 INTRODUÇÃO

Conforme abordado na Parte 1 do Guia de Boas Práticas, os dados dos colaboradores do Sistema Indústria podem ser utilizados para diferentes fins e em diferentes fases: (i) pré-contratual, como currículos e cartas de motivação; (ii) contratual, como exames admissionais e informações pertinentes à contratação; (iii) execução contratual, como registro de jornada e administração da folha de pagamento; e (iv) pós-contratual, com armazenamento e exclusão dos dados conforme prazo prescricional.

Os colaboradores compõem uma importante categoria de titulares e que comumente têm seus dados sensíveis tratados, desde a coleta em processos seletivos e posteriormente com a relação trabalhista desenvolvida. Além disso, são diversos os dados e operações de tratamento de dados envolvidos na gestão de pessoas.

CICLO DE VIDA DOS DADOS NA GESTÃO DE PESSOAS

- **Fase pré-contratual**: a realização de processos seletivos requer a análise de currículos, cartas de motivação e são apresentadas informações na fase de entrevistas.
  - **Dados utilizados**: nome, endereço, *e-mail*, telefone, experiência profissional, formação acadêmica, informações sobre disponibilidade para trabalho no sábado (pode incluir dados sensíveis sobre religião), certidão de antecedentes criminais, etc.
- **Processo de contratação**: a contratação do(a) colaborador(a) requer a coleta de informações necessárias para elaboração do contrato de trabalho.
  - **Dados utilizados**: nome, data de nascimento, RG, CPF, CNH, CTPS, foto 3X4, endereço, telefone, *e-mail*, grau de escolaridade, número de registro no conselho profissional, naturalidade, nacionalidade, etnia, comprovante de residência, certificado militar, biometria, PIS/Pasep, passaporte, dados de saúde (p.ex. carteira de vacinação, laudo com comprovação de deficiência), exames admissionais, exames complementares (por exemplo, teste de audição), etc.
- **Execução do contrato de trabalho:** a execução do contrato de trabalho é processo contínuo que pode demandar uma multiplicidade de dados pessoais para diferentes formas de tratamento. De forma geral, o empregador irá acompanhar o desempenho do(a) colaborador(a), devendo cumprir com suas obrigações trabalhistas, assim como garantir a segurança do ambiente de trabalho. Esses processos podem utilizar tecnologias de administração de folha de pagamento, de ponto, etc.
  - **Dados de controle de ponto:** nome completo, RG, CPF, PIS, Endereço, data de nascimento, sexo (M/F), impressão digital (biometria), atestados médicos, etc.

  - **Dados para procedimentos financeiros:** nome completo, CPF, conta, agência, Banco, Conta FGTS, Tipo de conta, relatório de horas trabalhadas, informações sobre horário de entrada e saída, crédito consignado, informações sobre filiação, etc.
  - **Dados para concessão de benefícios:** nome completo, CPF dos filhos e cônjuge, Pessoa com Deficiência (PcD), saúde ocupacional, atestados, licenças, pensionista, gravidez, certidão de nascimento dos filhos, certidão de casamento ou comprovação de união estável e carteira de vacinação dos filhos, etc.
  - **Dados de utilização de equipamentos:** *cookies*, IP, localização, *wi-fi*, *bluetooth*, registros de *downloads*, assinaturas de *e-mail*, telefone, *e-mail*, etc.
  - **Dados para segurança no ambiente de trabalho:** câmeras de segurança, cadastro biométrico, dados cadastrais de visitantes (nome, CPF, RG, foto), carteira de vacinação, etc.

- **Encerramento da relação trabalhista**: após o encerramento da relação trabalhista diversos documentos e informações que contêm dados pessoais devem ser armazenadas por períodos determinados tanto pela existência de obrigações legais, quanto pela existência de processos trabalhistas em curso ou cujo prazo prescricional ainda não findou.
  - **Dados armazenados:** informações relativas ao FGTS (guia recolhimento do FGTS e informações à previdência social GFIP); – guia de recolhimento rescisório do FGTS e da contribuição social (GRFC); contribuição previdenciária, folha de pagamento, etc.

O tratamento de dados para a gestão de pessoas possui uma particularidade no Sistema Indústria tendo em vista a possibilidade de compartilhamento dos dados entre entidades do sistema pelas áreas compartilhadas, a depender da diretoria ou departamento ocupado pelo colaborador. Ademais, podem ser compartilhados dados com terceiros para realização de cursos ou para a própria gestão de sistemas de administração de pessoal.

Qualquer que seja a finalidade do tratamento dos dados dos colaboradores, fato é que as operações de tratamento devem cumprir com as condições de legitimidade para o tratamento de dados pessoais, devendo existir uma base normativa que autorize o tratamento e devendo ser respeitados os princípios da legislação.[83]

Entretanto, é certo que sempre que o empregador optar por realizar essa coleta de dados no ambiente de trabalho, em obediência ao princípio da transparência, os colaboradores devem ser avisados a que tipo de monitoramento estarão sujeitos.

5.2 CONDIÇÕES DE LEGITIMIDADE PARA O TRATAMENTO DE DADOS

Entre as possíveis bases legais para o tratamento desses dados, destacam-se as de cumprimento de obrigação legal ou regulatória, execução ou criação de contrato de trabalho. Em ambos os casos, não é necessário o consentimento dos colaboradores, abarcando inclusive as obrigações relativas ao contrato de trabalho e a outras normas que regulam a relação de emprego, como convenções coletivas.

83 SCHERTEL, Laura. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Panorama Setorial da Internet**, v. 11, n. 2, jun. 2019.

A coleta de consentimento para relações trabalhistas é, inclusive, aspecto controverso nas discussões sobre tratamento de dados no direito trabalhista, não sendo recomendável a utilização desta base legal. De acordo com o posicionamento do *Article 29 Working Party* – WP29,[84] a existência de relação hierárquica pode comprometer a "liberdade" no fornecimento do consentimento.

Assim, apresentamos algumas bases legais aplicáveis a cada uma das fases do tratamento de dados na gestão de pessoas.

Fase pré-contratual

- **Execução de contrato**: apesar de se tratar de momento pré-contratual, a base legal da execução do contrato pode se aplicar à coleta de currículo e entrevista, uma vez que o titular é parte da relação e o objetivo é celebrar um contrato caso a fase preliminar seja bem-sucedida.

Processo de contratação

- **Execução de contrato**: nesse momento, o titular é parte efetiva do contrato e as informações coletadas devem ter como objetivo celebrar a relação entre empresa e colaborador(a) – ainda que não seja de natureza trabalhista.
- **Legítimo interesse**: atividades de tratamento de dados como a exigência de antecedentes criminais, etc. não estão diretamente vinculadas à hipótese de execução do contrato por não serem realizadas a pedido do titular, mas podem ser enquadradas na base legal do legítimo interesse.

Execução do contrato

- **Execução de contrato**: a execução contratual pode ser utilizada como base legal apenas em relação à finalidade específica do contrato de trabalho, cuja impossibilidade de tratar o dado impediria a execução do contrato. Essa base pode ser utilizada para atividades como o pagamento do salário.
- **Legítimo interesse**: atividades de tratamento de dados como o acompanhamento de desempenho do(a) colaborador(a), etc. não estão diretamente vinculadas à hipótese de execução do contrato, por não serem realizadas a pedido do titular, mas podem ser enquadradas na base legal do legítimo interesse.
- **Cumprimento de obrigação legal ou regulatória**: as atividades de gestão de pessoas por vezes envolve o tratamento de dados que devem ser armazenados para cumprimento de obrigações fiscais e trabalhistas, por forma de leis como a Lei nº 8.036/1990 (FGTS), CLT, CTN, etc.

Encerramento da relação

- **Cumprimento de obrigação legal ou regulatória**: mesmo após o encerramento da relação trabalhista, os empregadores devem armazenar dados, como o guia recolhimento do FGTS e informações à previdência social (GFIP); guia de recolhimento rescisório do FGTS (GRFC) e da contribuição social por conta de obrigações expressas no CTN, CLT, etc.
- **Exercício regular de direitos**: as relações trabalhistas recorrentemente são objeto de disputas judiciais. Assim, até que os prazos prescricionais finalizem e os processos sejam arquivados de forma definitiva, dados essenciais para subsidiar essa disputa podem ser armazenados. É possível, ainda, e até comum na prática, a empresa precisar comprovar o tempo de serviço do colaborador em processo judicial para fins de aposentadoria, fato que pode se dar muitos anos após o prazo prescricional de uma reclamação trabalhista.

84 Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade, cujas atribuições estão previstas no art. 30.º da Diretiva 95/46/CE e no art. 15.º da Diretiva 2002/58/CE.

Cumpre ressaltar que a utilização de cada uma das bases legais depende do contexto específico no qual ela seja aplicada e, por isso, o enquadramento da operação de tratamento deve sempre ser acompanhado dos outros princípios norteadores da legislação. Deve-se ter especial atenção ao princípio da finalidade, necessidade e adequação, uma vez que independentemente da existência de contrato ou obrigação legal, o tratamento de dados deve ser realizado quando os dados forem pertinentes, adequados e limitados aos fins para os quais são processados.

Observa-se que, antes da fase contratual e após a rescisão do contrato de trabalho, o controlador dos dados, quem realiza a contratação, contará com o poder decisório sobre o tratamento dos dados pessoais dos empregados, em especial quanto à coleta.

Por isso, devem-se evitar práticas excessivas, como a solicitação de exames admissionais não compatíveis com o cargo pretendido. Além do mais, não se pode desconsiderar existência de normas legais e regulatórias que incidem sobre a coleta de dados a depender das finalidades formalmente instituídas para o seu tratamento, motivo pelo qual é necessária atenção para garantir que os dados coletados e tratados serão apenas o mínimo necessário para cumprimento dessas obrigações.

No tocante à coleta de currículos e demais documentos, é recomendável que se informe aos candidatos a intenção em deixar seus dados em cadastro de reserva e qual seria o período definido para este fim, com manifestação específica e clara. Destaca-se que para o tratamento de dados sensíveis, que envolvam condições de saúde, por exemplo, pode ser necessária a coleta de consentimento. Contudo, a avaliação sobre a necessidade de tratamento deste dado deve ser realizada com maior rigor, especialmente considerando aqueles dados que podem colocar, em risco, direitos e liberdades dos titulares ou expô-los a discriminações abusivas ou ilegais.

Especialmente quando dados sensíveis estiverem envolvidos – como no caso de gestão de planos de saúde, exames admissionais, etc. –, as medidas de controle de acesso, as técnicas de pseudonimização e a elaboração de Relatório de Impacto devem ser adotadas. Por exemplo, em vez de no sistema constar o nome completo dos indivíduos, podem ser identificados inicialmente pelos números funcionais, com controle de acesso às informações completas.

Dados de identificação, como os presentes em crachás, também devem seguir a base principiológica da LGPD. Nesse sentido, se a entrada dos funcionários ocorre pela verificação do nome dos colaboradores, não é recomendável que neste documento contenha outros dados pessoais que dependem da apresentação de outro documento para a sua validação, como é o caso do CPF ou RG. Mesmo a utilização de foto nos crachás pode ser reavaliada se a validação de identidade é feita por meio de sistemas informatizados.

Por fim, para evitar que, por exemplo, homônimos sejam confundidos, outras medidas adicionais de identificação podem ser utilizadas, como a utilização de número funcional ou então o registro de fotos apenas no sistema de verificação, para que o reconhecimento seja realizado.

6 PROTOCOLO PARA A ELABORAÇÃO DE ACORDOS ENTRE AGENTES DE TRATAMENTO

6.1 INTRODUÇÃO

Conforme apresentado na Parte 1 deste guia, os agentes de tratamento, o controlador e o operador podem ser pessoas natural ou jurídica, de direito público ou privado, sendo figuras essenciais para o ecossistema de proteção de dados pessoais.

As situações nas quais uma pessoa física assume o papel de agente de tratamento são específicas e terão um tratamento diferenciado definido pela ANPD. Nos cenários mais corriqueiros, por sua vez, uma pessoa jurídica irá ocupar as funções dos agentes de tratamento. Nesses casos, a organização assumirá o papel, não sendo necessária a representação por qualquer funcionário ou sócio da empresa,[85] ou seja, uma organização pode desenvolver o papel de operador em determinado tratamento que envolve outra organização e, em outro processo, esses papéis podem ser invertidos. Esse é mais um dos motivos que justificam a necessidade de manutenção de **registro das operações** de tratamento de dados realizadas (art. 37 da LGPD), obrigação compartilhada por ambos os agentes de tratamento.

Ademais, existe a figura do suboperador, agente contratado pelo operador para participar do tratamento de dados definido pelo controlador. Portanto, não há relação direta entre o controlador e o suboperador, apesar de estarem envolvidos no mesmo tratamento. Para fins de responsabilidade, o suboperador é equiparado ao operador e, por isso, segue a mesma lógica do art. 42, §1º, I, da LGPD: caso descumpra as determinações do operador ou do controlador, o suboperador passará a atuar como controlador e responderá como

85 BRASIL. Autoridade Nacional Proteção de dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 6 ago. 2021.

controlador. Vale destacar que, em princípio, a mera existência deste agente não é suficiente para caracterizar a controladoria conjunta, pois ele não atua na determinação dos elementos essenciais para o tratamento de dados, como será abordado adiante.

A relação entre os agentes de tratamento de cada tratamento, muitas vezes, é definida contratualmente, mas a efetiva identificação de cada agente será determinada pelas funções desempenhadas por cada um, objeto de considerações no próximo item (VI.2. Definição de papéis).

Dessa maneira, a definição dos papéis dos agentes de tratamento e o estabelecimento de condições por meio de contratos podem ser importantes aspectos para a redução da exposição do controlador. Tal fato decorre da maior carga de responsabilidade que o controlador possui em relação à comprovação do cumprimento com os termos da legislação, assim como na garantia dos direitos dos titulares.

Por esse motivo, o controlador tem papel estratégico na definição da atuação do operador, sendo o contrato um instrumento importante para a definição das obrigações dos operadores e os limites da atuação dos subcontratadores.[86]

6.2 DEFINIÇÃO DE PAPÉIS

O papel desempenhado por cada agente em determinado tratamento de dados é essencial para fins de responsabilidade e para compreender quais são as obrigações de cada entidade envolvida naquela cadeia de tratamento. Essa definição pode ser formalizada por meio de um contrato, contudo, o efetivo desempenho das funções é essencial para identificação do papel de cada agente de tratamento. Isso porque a LGPD define diferentes encargos aos diferentes agentes de tratamento. Algumas dessas atribuições são comuns a todos os agentes, mas outras são específicas para cada papel, devido às peculiaridades de sua atuação.[87]

Do mesmo modo, é possível que a relação entre os agentes de tratamento de cada tratamento seja definida por meio de outras formas de interação empresarial. Contudo, independentemente de acordos estabelecidos entre os agentes de tratamento, o que é essencial para determinar se uma organização está atuando como controladora dos dados é justamente o **poder de decisão** sobre os tratamentos realizados.

86 EUROPEAN DATA PROTECTION BOARD - EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR.** jul. 2021. Disponível em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: 22 jun. 2023.

87 LAPIN. **Cartilha controlador ou operador: quem sou eu?** Disponível em: https://lapin.org.br/2021/04/09/cartilha-controlador-ou-operador-quem-sou-eu/

Para a caracterização do mencionado poder decisório, é necessário o controle sobre os elementos essenciais do tratamento, como a definição da finalidade do tratamento, da natureza dos dados pessoais tratados e a duração do processo.[88] Portanto, situações como a definição de papéis em contrato que seja incompatível com as responsabilidades reais do agente de tratamento, ou a excessiva atribuição de responsabilidades ao operador quando não é ele o tomador de decisão, não são resguardadas à luz da legislação.

Ainda existe a controladoria conjunta, caracterizada por situações em que existem dois ou mais responsáveis pelo tratamento, ou seja, mais de um agente participa da determinação dos elementos essenciais daquele tratamento. As decisões conjuntas podem ser tomadas a partir de uma atuação comum, em que há verdadeira atuação conjunta, ou por meio de decisões convergentes que, apesar de distintas, são complementares. Nos casos em que restar comprovada a controladoria conjunta, haverá responsabilidade solidária dos controladores, conforme disposição do art. 42, §1º, II, da LGPD.[89]

Dessa forma, em caso de atuação do operador fora do escopo das determinações do controlador em relação aos elementos essenciais do tratamento, o operador atua como verdadeiro controlador. Isso afasta as responsabilidades do suposto controlador sobre aquele tratamento e as traz para o operador atuando como controlador, de tal forma que esse deverá cumprir com todas as obrigações do controlador (art. 42, §1º, I, da LGPD).

Por exemplo, é possível indicar que as entidades do Sistema Indústria, como o Sistema SESI e o SENAI, embora cada um corporifique órgãos normativos e órgãos de administração, de âmbito nacional e de âmbito regional, os órgãos regionais respectivos gozam de autonomia financeira e administrativa, para execução dos seus serviços e objetivos.

88 BRASIL. Autoridade Nacional Proteção de dados. **Guia orientativo para definições dos agentes de tratamnto de dados pessoais e do encarregado**. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 6 ago. 2021.

89 BRASIL. Autoridade Nacional Proteção de dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 6 ago. 2021.

Atenção!

- Cada pessoa jurídica do Sistema Indústria pode atuar como operador e controlador, a depender do tratamento e do contexto. Por essa razão, os instrumentos jurídicos dirão respeito a tratamentos específicos, a fim de determinar o papel de cada agente naquele processo
  - A CNI pode atuar como **controladora** nas atividades voltadas à defesa de interesses da indústria perante o Executivo Federal.
  - O SENAI pode atuar como **controlador** em atividades como a Concessão de Bolsas de Estudos.
  - O SESI, por sua vez, pode atuar como **operador** nas hipóteses em que é contratado para oferecer algum serviço que será personalizado de acordo com as indicações do cliente em contrato. Um exemplo é o Sistema S+ (SESI Viva+), [90] *software* de gestão contratado por empresas, que são as responsáveis pela definição das finalidades das operações de tratamento de dados pessoais.
  - O IEL pode ser **controlador** nas atividades relativas à oferta de cursos de educação executiva e nos cursos Inova Talentos.

Nesse sentido, destacamos os deveres de cada um dos agentes de tratamento, assim como aqueles que são comuns aos operadores e controladores:

Deveres comuns aos agentes de tratamento

- Conformidade com os **princípios** da LGPD.
- Implementação de **medidas de segurança técnicas e organizacionais.**
- **Registro** de operações de tratamento de dados pessoais.
- Observância das regras de **transferências internacionais.**

Obrigações dos controladores

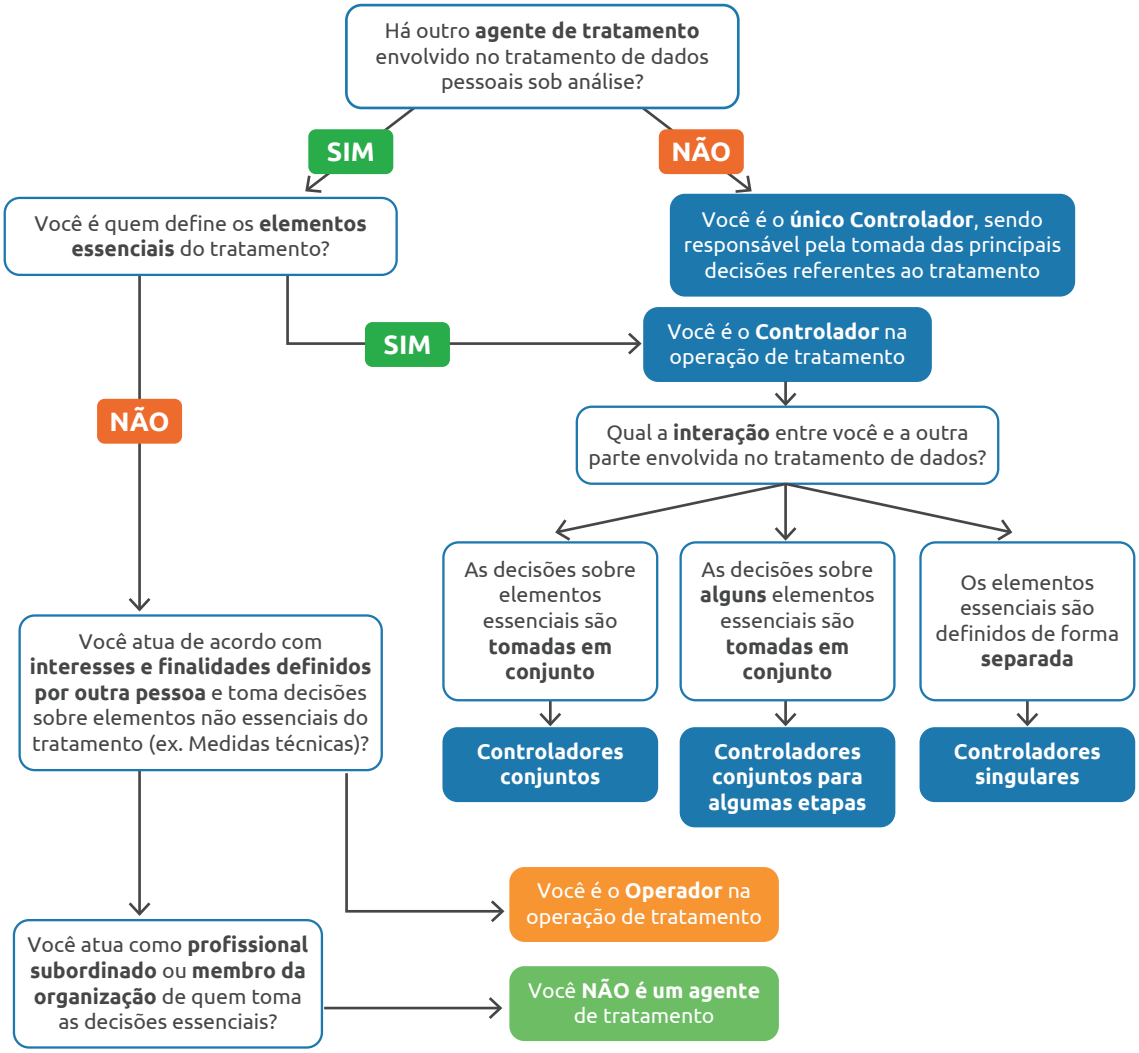
- Manutenção do **ônus da prova** de que o consentimento do titular foi obtido em conformidade com a LGPD.
- Observância dos **direitos dos titulares**.
- **Comunicação de incidentes de segurança que possam acarretar risco ou dano relevante** à ANPD e aos titulares afetados.
- Elaboração de **Relatório de Impacto de Proteção de Dados**.
- Nomeação de **encarregado** de dados**.**
- Implementação de **programa de governança em privacidade** com os requisitos previstos no art. 50, §2º.

Obrigações dos operadores

- Cumprir com as **instruções do controlador** sobre o tratamento de dados.
- **Notificar** de incidentes de segurança ou possível violação de proteção de dados ao controlador.
- **Reparar os danos causados** em razão do exercício de atividade de tratamento de dados pessoais, **quando este descumprir com suas obrigações ou não seguir as orientações do controlado**r.

90 O *software* é desenvolvido com o intuito de fornecer melhores condições para tomada de decisões das empresas por meio da unificação de informações sobre obrigações fiscais, previdenciárias e trabalhistas, facilitando e agilizando os envios de eventos SST para o e-Social com controle de acesso facilitado e segurança dos dados.

Para auxiliar a aplicação dos conceitos de controlador e operador, a ANPD divulgou o seguinte fluxograma[91] na versão mais recente (maio/2022) do Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado:



6.3 ELABORAÇÃO DE CLÁUSULAS CONTRATUAIS

Conforme mencionado, ainda que a identificação do papel de cada um dos agentes pelo contexto fático da relação, a definição de papéis pode ser formalizada por meio de contratos. A inclusão de cláusulas contratuais pode ser importante para o estabelecimento das obrigações de cada parte e definição das instruções sobre procedimentos a serem adotados, por exemplo, em incidentes de segurança.

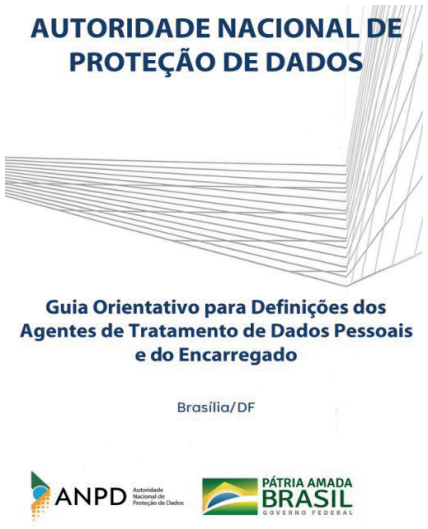
91 Fluxograma do **Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado ANPD** reproduzido de forma resumida.

Contudo, conforme exposto anteriormente, é necessário ressaltar que a efetiva identificação dos papéis dos agentes de tratamento decorre do contexto fático. Assim, ainda que um contrato estabeleça quem é o controlador e quem é o operador, a avaliação dos papéis efetivamente assumidos será determinante para a avaliação das responsabilidades de cada um dos agentes.

De acordo com o guia do EDPB,[92] os contratos podem contribuir para o balanceamento das posições negociais e podem ser importante mecanismo de garantia de cumprimento com a legislação de proteção de dados. O órgão recomenda, portanto, que o contrato não se restrinja aos termos da legislação, levando em consideração as responsabilidades das partes, o nível de segurança que é exigido no tratamento de dados realizado, confidencialidade da matéria tratada, assim como deve prever informações sobre o risco envolvido no tratamento de dados realizado sob o contrato em questão.[93]

Também é possível definir os limites das funções de cocontroladores, podendo ser definidas as decisões comuns (duas empresas decidem em conjunto as finalidades e meios de tratamento) ou decisões convergentes (decisões distintas, mas complementares) por meio do instrumento contratual.

Dessa forma, mesmo que a responsabilização dos agentes de tratamento seja avaliada contextualmente pela ANPD, a elaboração de cláusulas contratuais pode auxiliar no estabelecimento do regime de atividades e as responsabilidades de cada parte. Nos termos do **Guia de Agentes de Tratamento da ANPD**:



"Ainda que a LGPD não determine expressamente que o controlador e o operador devam firmar um contrato sobre o tratamento de dados, tal ajuste se mostra como uma boa prática de tratamento de dados, uma vez que as cláusulas contratuais impõem limites à atuação do operador, fixam parâmetros objetivos para a alocação de responsabilidades e reduzem os riscos e as incertezas decorrentes da operação.

Os pontos que podem ser definidos contratualmente são o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos e obrigações e responsabilidades relacionados ao cumprimento da LGPD." (p. 16)

92 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR.** jul. 2021. p. 34. Disponível em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: 22 jun. 2023.

93 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR.** jul. 2021. p. 34. Disponível em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: 22 jun. 2023.

Assim, sugerimos que a elaboração de cláusulas contratuais considere os seguintes tópicos:

- Glossário com terminologia da LGPD.
- Duração das atividades de tratamento.
- Indicação de agentes de tratamento.
- Finalidades específicas do tratamento de dados.
- Vedação à utilização de dados pessoais sem ciência ou autorização da controladora.
- Exigência de adequação das partes do contrato à LGPD.
- Vedação ao compartilhamento de dados pessoais e obrigatoriedade de notificação à parte caso o compartilhamento seja necessário.
- Obrigação de registro de informações.
- Obrigação de implementação de medidas técnicas e administrativas que garantam a segurança dos dados tratados.
- Identificação da categoria dos titulares de dados pessoais envolvidos na atividade de tratamento.
- Possibilidade de realização de auditorias para demonstração de cumprimento da legislação.
- Deveres de confidencialidade.
- Periodicidade de atualização de informações do contrato.
- Hipóteses de transferência de dados, inclusive internacional.
- Obrigatoriedade de elaboração de plano de incidentes envolvendo dados pessoais.
- Procedimentos de destruição e devolução de dados pessoais.
- Obrigatoriedade de notificação em caso de determinações oficiais que obriguem o fornecimento de dados pessoais.
- Obrigatoriedade de contratação de encarregado por operador.

6.4 CONTRATAÇÃO DE PARCEIROS E EMPRESAS TERCEIRIZADAS

Por vezes, a complexidade das relações empresariais exige a contratação de empresas terceirizadas para o auxílio no desempenho de determinadas atividades. Quando essas atividades envolverem o tratamento de dados pelo operador, as empresas terceirizadas serão caracterizadas como suboperadores.

O suboperador é o agente contratado pelo operador para participar do tratamento de dados definido pelo controlador, então não há relação direta entre o controlador e o suboperador, apesar de estarem envolvidos no mesmo tratamento. Insta ressaltar que para fins de responsabilidade, o suboperador é equiparado ao operador, então segue a mesma lógica do art. 42, §1°, I, da LGPD – se descumprir as determinações do operador/controlador, o suboperador passará a atuar como controlador e responderá como controlador.

Assim, recomenda-se que os contratos estabeleçam cláusulas que impeçam que a contratação de suboperadores ocorra sem anuência prévia do controlador e que vedem o compartilhamento de dados pessoais com outros parceiros comerciais que não estão envolvidos na relação. Ademais, no caso de contratação de outro operador de dados, é necessário garantir que este agente esteja submetido às mesmas condições que o operador, incluindo a possibilidade de se realizar auditorias para garantir o cumprimento dos termos do contrato.[94]

94 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR.** jul. 2021. p. 37. Disponível em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: 22 jun. 2023

7 PROTOCOLO PARA UTILIZAÇÃO DE APARELHOS PRIVADOS E SISTEMA DE MENSAGERIA PRIVADA PARA FINS INSTITUCIONAIS

7.1 INTRODUÇÃO

Não se pode ignorar que os diferentes meios de comunicação são utilizados pelas entidades e seus colaboradores, motivo pelo qual os dados compartilhados nessas trocas devem ser objeto de adequação à LGPD, como prevenção a possíveis incidentes como o vazamento de informações não permitidas.

Os meios institucionais adotados no âmbito das entidades e órgãos nacionais são o *e-mail*, a Plataforma *Microsoft Teams* e a Plataforma CRM (*Customer Relationship Management*). Além disso, é comum o uso do *WhatsApp* para facilitação do contato entre os participantes no âmbito do Sistema Indústria.

A utilização de plataformas pelos colaboradores e atores relacionados ao Sistema Indústria merece especial atenção, uma vez que esses sistemas conectam milhares de pessoas de todas as entidades. Assim, serão apresentadas algumas recomendações que já são adotadas pelas entidades e órgãos, bem como pontos de atenção na utilização desses sistemas.

7.2 TROCA DE MENSAGENS POR MEIO DE PLATAFORMAS DIGITAIS – *MICROSOFT TEAMS* E WHATSAPP

Inicialmente, destacamos a importância da realização de treinamentos constantes com os colaboradores sobre temas atinentes à proteção de dados, como o manuseio de informações pessoais, o descarte de documentos ou mesmo sobre a avaliação da necessidade de se coletar determinadas informações pelos colaboradores responsáveis pelo atendimento ao público. Esse tipo de iniciativa pode ser fundamental para que informações relacionadas a dados pessoais não sejam compartilhadas de forma irrestrita.

Fique atento!

- Independentemente do aplicativo de mensageria utilizado, os colaboradores devem receber instruções a respeito das medidas de segurança e proteção de dados pessoais no uso dessas ferramentas de comunicação, preferencialmente documentada em cartilhas ou demais materiais internos.
- Mesmo que alguns aplicativos disponham de medidas como a criptografia de ponta a ponta e verificação em duas etapas, não é garantido o bloqueio razoável contra golpistas e *hackers* mal-intencionados, os quais podem acessar não apenas os conteúdos da vítima, como toda a rede de contatos que possui. Assim, é essencial realizar periodicamente treinamentos para conscientização dos colaboradores sobre golpes comuns na internet e sobre cuidados que são necessários na navegação *on-line*.

Determinadas atividades podem ser registradas por meio de fotos, vídeos, gravações de áudios e *Printscreen*. Contudo, tais informações podem conter informações pessoais sensíveis com alto potencial de exposição do titular. Assim, na utilização das plataformas digitais para fins institucionais, deve-se evitar ao máximo o compartilhamento de informações que contém dados pessoais, especialmente quando se tratar de plataformas não reconhecidas institucionalmente, mas que podem ser utilizadas para tais fins.

Outro exemplo refere-se às fotos que ocorrem em eventos institucionais e podem ser compartilhadas com o intuito de promovê-lo. Contudo, não se recomenda que sejam tiradas fotos que possam registrar informações sensíveis como a tela de trabalho, muito menos que sejam publicadas nas redes sociais dos colaboradores, pois esse tipo de comportamento pode facilitar o vazamento de informações e dados pessoais.

Com relação à utilização de plataformas de mensagens, sugere-se que os *e-mails* corporativos e aplicativos de mensageria oficiais das entidades sejam priorizados. Ademais, os aparelhos celulares utilizados para a comunicação interna e externa da organização devem possuir o sistema de **verificação em duas etapas**, sendo incluída uma camada extra de segurança à conta cadastrada.

Entre os aplicativos existentes, é observado que o WhatsApp é comumente utilizado e, atualmente, não é mais restrito a conversas entre amigos ou famílias, sendo uma das principais formas de comunicação dos consumidores com empresas,[95] visto que o aplicativo conta com gratuidade e diferentes funcionalidades para as conversas. Ainda assim, o uso do WhatsApp não deve ser prioritário para as instituições.

O uso de grupos nestes aplicativos de mensageria instantânea também podem envolver nomes, números, fotos e várias outras informações de contato, que podem alcançar centenas de indivíduos ao mesmo tempo. Esses dados, em princípio, não possuem o potencial de gerar grandes riscos aos usuários, mas exigem das instituições o cuidado em

95 MATSUE, Carla. 80% dos brasileiros utilizam o WhatsApp para se comunicar com as marcas, aponta pesquisa. **Valor Investe**. Disponível em: https://valorinveste.globo.com/objetivo/gastar-bem/noticia/2021/09/16/80percent-dos-brasileiros-utilizam-o-whatsapp-para-se-comunicar-com-as-marcas-aponta-pesquisa.ghtml. Acesso em: 22 jun. 2023.

garantir que as pessoas consentem em serem inseridas. Isto pode ser providenciado por meio do compartilhamento do *link* temporário de convite para ingresso no grupo com a pessoa,[96] bem como o fornecimento de orientações sobre as finalidades e uso adequado desses meios.[97]

Ademais, recomendamos as seguintes orientações práticas para a utilização de aplicativos de mensageria instantânea:

Orientações para utilização de aplicativos de mensageria instantânea

- Ative as medidas de segurança dos aplicativos, como a autenticação de dois fatores e o uso de senhas que somente serão utilizadas nos aplicativos de mensagens.
- Se você usar o aplicativo apenas no celular, desative a função de *download* automático de fotos e vídeos recebidos.
- Caso utilize o aplicativo em um computador:
  - Use apenas aplicativos oficiais.
  - Certifique-se de que não deixou seu perfil logado ao desligar o computador.
  - Evite acessar o aplicativo em computadores ou redes públicas.
  - Não baixe arquivos ou clique em *links* de fontes não confiáveis, especialmente se vierem de contatos desconhecidos.
  - Mantenha os aplicativos e antivírus atualizados em seu computador.
- Não compartilhe informações de contato, como números de telefone, com terceiros sem autorização.
- Tenha cautela ao expor fotos no perfil das plataformas digitais usadas para troca de mensagens, especialmente aquelas que envolvem outras pessoas, como menores de idade. Isso evita exposição indesejada e o acesso não autorizado a essas informações.
- Tenha cuidado ao encaminhar mensagens, limitando as conversas em grupos e chats profissionais aos assuntos relevantes.
- Se não tiver certeza sobre a veracidade de uma mensagem ou quem a escreveu, evite encaminhá-la. Essa postura é recomendada para evitar o compartilhamento de conteúdos desinformativos.
- Ative o bloqueio remoto do celular para evitar o uso indesejado por terceiros em caso de perda ou roubo, caso o recurso esteja disponível.

7.3 PLATAFORMA CRM

A Plataforma CRM pode ser compreendida como um *software* de armazenamento e gerenciamento de informações. A base de dados conta com informações de alunos, ex-alunos, discentes, empregados contratados, parceiros temporários, personalidades com quem o Sistema Indústria mantém algum tipo de relacionamento.

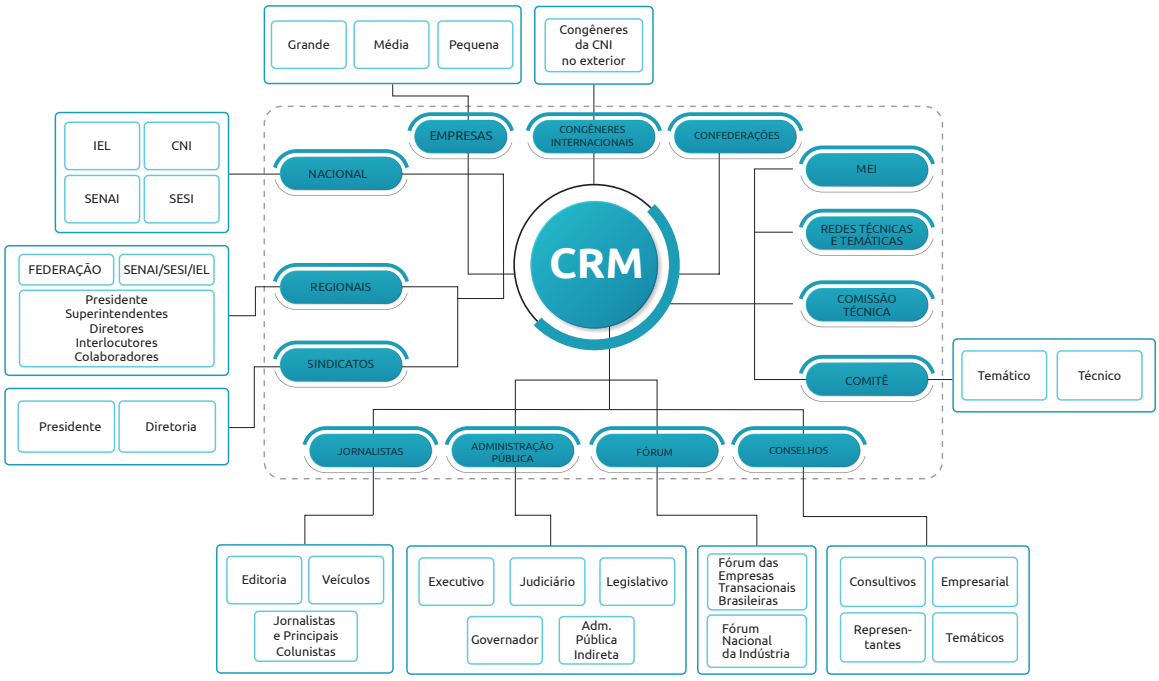
96 PRIDATECT. **How to comply with the GDPR if you use WhatsApp in your company?** 2021. Disponível em: https://www.pridatect.co.uk/blog/2021/10/27/how-to-comply-with-the-gdpr-if-you-use-whatsapp-in-your-company/. Acesso em: 26 jun. 2023.

97 MRS. **GDPR in practice n. 1**: using WhatsApp in compliance with GDPR. 2020. Disponível em: https://www.mrs.org.uk/pdf/GDPR%20In%20Practice%20Vol%201%20WhatsApp%20in%20compliance%20with%20GDPR.pdf. Acesso em: 26 jun. 2023.

A plataforma é utilizada pelo Sistema Indústria para facilitar a comunicação, gestão de projetos e o atendimento a diversas funções institucionais que envolvem contato com terceiros e possibilita o registro de dados de contatos internos e externos, além do gerenciamento da comunicação por meio do agendamento de reuniões via *e-mail* ou ligação telefônica, por exemplo.

O Sistema Indústria conta com dois documentos importantes que vinculam as entidades e órgãos nacionais: **Normas e Políticas de Uso do CRM** e **Governança de Dados do CRM**. Ambos documentos devem ser acessados quando do tratamento de dados pessoais por meio do sistema para garantir a melhor gestão de dados na plataforma.

A importância dessa plataforma no Sistema Indústria decorre de sua centralidade e da quantidade de atores envolvidos na plataforma. Do esquema seguinte, é possível identificar os seguintes grupos de agentes: i) Diretoria Nacional da CNI e IEL; ii) Diretorias regionais das federações; iii) Departamentos Regionais do SESI e SENAI; iv) federações; v) sindicatos; vi) jornalistas; Administração Pública; fóruns (Fórum das Empresas Transnacionais Brasileiras e Fórum Nacional da Indústria); vii) conselhos (Consultivo, Empresarial, Representantes; Temáticos); viii) comitê (temático e técnico); ix) comissão técnica; redes técnicas e temáticas; x) MEI; xi) confederações; xii) entidades congêneres da CNI no exterior; e xiii) Empresas.[98]



Fonte: Governança de dados do CRM (CNI).

98 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Governança de dados do CRM**. 2. ed. Brasília: CNI, 2020. p. 18.

De acordo com o previsto no documento sobre Governança de Dados do CRM, são armazenados dados – incluindo dados pessoais – para as mais diversas finalidades. Entre elas, destacamos gestão de dados que podem ser tratados para:[99]

Atividade	Dados
Registro de contato	Tipo de contato, tratamento, nome completo, codinome, telefone, celular, *e-mail* comercial, empresa/entidade, cargo, departamento, endereço, UF de eleição, cidade de nascimento, Estado de Nascimento, Vocativo, Partido, CPF, Estado Civil, aniversário, sexo, Parlamentar, redes sociais (*Facebook*, *Linkedin*, *Instagram*), etc.
Prospecção de clientes, oferta de serviços e registros de contratos, mapeamento de oportunidades, etc.	Nome completo, telefone, *e-mail*, tópico de interesse, etc.
Realização de campanhas de defesa de interesses e interação com o público alvo	Telefone, *e-mail*, carta, fax, etc.
Criação de Conexões corporativas (funcional) ou pessoais (particular)	Nome do contato, tipo de conexão, forma de conexão, etc.
Gestão de grupos temáticos que se reúnem por periodicamente para tratar assuntos de interesse da indústria	Tipo e grupo, nome, classificação (interno ou externo), participantes do grupo, etc.
Envio de campanhas de *marketing* para contatos, clientes ou clientes em potencial	Nome, tipo de lista, descrição, etc.
Atendimento de ocorrências, solicitações, demandas, reclamações	Cliente, instituição, descrição da ocorrência, complexidade, etc.

A principal medida de segurança em relação ao uso da ferramenta CRM é o alto padrão de controle de acesso. O *software* só pode ser acessado por meio de um *login* e senha único de cada usuário. As senhas devem ser modificadas periodicamente e existem diversas regras para evitar a repetição das palavras de segurança.

Cada usuário tem acesso limitado aos perfis as informações estritamente necessários para as finalidades desenvolvidas pela sua área. Além disso, existem informações que somente serão acessíveis pelo gerente de determinado setor e somente com a autorização deste superior outros usuários poderão acessar esses perfis.

Para garantir que dados desnecessários não sejam armazenados, o sistema CRM dispõe de um ciclo básico de limpeza anual dos dados armazenados, que envolve:[100]

- Qualificação – é o processo que tem por objetivo complementar determinadas informações de um cadastro com fim específico.
- Higienização – como o próprio termo sugere, visa tornar a base de dados mais "limpa". Isso significa remover duplicidades de registros, enriquecer informações, identificar e remover dados incorretos do banco de dados.

99 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Governança de dados do CRM.** 2. ed. Brasília: CNI, 2020. p. 32-37; CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Normas & políticas de uso do CRM**. 2. ed. Brasília: CNI, 2020. p. 37-57.

100 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Normas & políticas de uso do CRM.** 2. ed. Brasília: CNI, 2020. p. 12.

- Eliminação – caso o titular dos dados pessoais cadastrados na plataforma tenha solicitado a sua eliminação, nos termos do art. 18, inciso IV, da LGPD, a partir da solicitação, e não anualmente.

Já em relação às regras de duplicidade, o sistema possui as seguintes regras de avaliação:[101]

MÓDULO	REGRA DE DUPLICIDADE
Contato	• Contatos com o mesmo CPF
	• Contatos com o mesmo nome completo + *e-mail*
	• Contatos com o mesmo nome completo + telefone principal + empresa
Pessoa Jurídica	• Pessoa Jurídica com o mesmo CNPJ
	• Tipo de Cliente = Internacional, será válido o nome da Empresa + País
Cliente Potencial	• *E-mail* + UF (Origem dos Portais do SI - Fale Conosco)
	• Nome completo + *e-mail*
Oportunidade	• Id da Oportunidade
	• Id da Oportunidade Regional
Produto da Oportunidade	• Id do Produto Existente
	• Produto Existente
Proposta	• Proposta com o mesmo ID Regional
Contratos	• Contratos com o mesmo ID Regional
Campanhas de *Marketing*	• Id da Campanha

Fonte: Normas e Políticas de Uso do CRM (CNI).

O que se observa da estrutura do CRM e dos documentos publicados é que a plataforma possui estrutura consistente de gestão de dados. Ainda assim, dada a quantidade de informações armazenadas, recomenda-se que sejam realizados treinamentos periódicos com os colaboradores e terceiros interessados a respeito das boas práticas que devem ser adotadas no manuseio do sistema.

Recomenda-se especial atenção para o atendimento dos princípios da LGPD. O princípio da necessidade ressalta que o tratamento deve ser restringir ao mínimo necessário para a realização de suas finalidades, estas as quais devem atender a propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I e III, da LGPD).

Ademais, para que o tratamento de dados seja considerado adequado e razoável, o princípio da adequação, previsto no art. 6º, II, da LGPD torna explícita a obrigatoriedade de que apenas dados imprescindíveis para alcançar os objetivos almejados sejam tratados, considerando o contexto do tratamento e a compatibilidade do tratamento de dados com a finalidade inicial que justificou a coleta dos dados.

101 *Idem, ibidem.*

Recentemente o Tribunal de Justiça Europeu[102] propôs cinco critérios para a avaliação de que uma nova finalidade é (ou não) compatível com a finalidade inicial que justificou a coleta e o tratamento de dados, a partir de um caso julgado. Em síntese, os critérios indicados são:

1. A possível existência de uma ligação entre as finalidades para as quais os dados pessoais foram recolhidos e as finalidades do tratamento posterior previsto.
2. O contexto em que os dados pessoais foram recolhidos, nomeadamente no que diz respeito à relação entre os titulares dos dados e o responsável pelo tratamento.
3. A natureza dos dados pessoais.
4. As possíveis consequências do processamento adicional previsto para os titulares de dados.
5. A existência de salvaguardas adequadas tanto no âmbito do tratamento inicial como do tratamento subsequente previsto.

Novamente, o contexto pelo qual o dado foi disponibilizado originalmente é uma importante base para a melhor avaliação que garanta os direitos dos titulares e a sua legítima expectativa quanto ao uso de suas informações (também em respeito ao princípio da boa-fé), bem como assegure a legalidade do tratamento posterior. Nesses casos, materializar o princípio da necessidade exige a ponderação em cada situação concreta, de forma lógica e suficientemente estreita entre as finalidades da coleta inicial de dados pessoais e o posterior tratamento desses dados.[103]

102 DROIT & TECHNOLOGIES. **RGPD**: ma nouvelle finalité est-elle compatible avec la finalité initiale? Disponível em: https://www.droit-technologie.org/actualites/rgpd-ma-nouvelle-finalite-est-elle-compatible-avec-la-finalite-initiale/. Acesso em: 26 jun. 2023.

103 DROIT & TECHNOLOGIES. **RGPD**: ma nouvelle finalité est-elle compatible avec la finalité initiale? Disponível em: https://www.droit-technologie.org/actualites/rgpd-ma-nouvelle-finalite-est-elle-compatible-avec-la-finalite-initiale/. Acesso em: 26 jun. 2023.

8 PROTOCOLO PARA TRATAMENTO DE DADOS PARA REALIZAÇÃO DE EVENTOS INSTITUCIONAIS

8.1 INTRODUÇÃO

Importante parte das atividades do Sistema Indústria é a promoção de eventos institucionais que visam aproximar o setor da sociedade e demais instituições, notadamente o setor privado e público. Esses eventos têm como objetivo promover os trabalhos realizados pelo Sistema, além de fomentar o debate de temas essenciais para o desenvolvimento da indústria.

Entre os eventos organizados pelas diferentes entidades do Sistema Indústria, podemos mencionar:

- Seminários.
- *Workshops*.
- Fóruns.
- Webinários.
- Reuniões técnicas.
- Reuniões de mecanismos.
- Reuniões de conselho.
- Eventos de missão prospectiva.
- Feiras.
- Eventos de missão comercial.
- Encontros de negócio.

A realização de eventos envolve o tratamento de dados como nome, *e-mail*, telefone, cargo, além de outras informações eventualmente coletadas no cadastro do contato na Plataforma CRM. Assim, é necessário apresentar alguns cuidados que as entidades do Sistema Indústria devem ter nas operações de tratamento de dados com essa finalidade, em especial considerando **três momentos principais para a realização de eventos institucionais**:

(ETAPA 1) PREPARAÇÃO DO EVENTO – ORGANIZAÇÃO E DIVULGAÇÃO DOS EVENTOS ANTES QUE ELES OCORRAM

Exemplos de dados tratados e finalidades:

- ***Dados cadastrais (nome completo, endereços de e-mail, números de telefone):*** Envio de convites para palestrantes, divulgação do evento, inscrição de participantes, contratação de fornecedores, elaboração de crachás e materiais personalizados.
- ***Dados relativos à profissão, ao nível educacional:*** análise do público-alvo e direcionamento de conteúdos personalizados depois da realização do evento, recebimento de inscrições para submissão de trabalhos científicos para o evento.
- ***Dados sobre participantes com necessidades especiais e dados sobre raça e gênero:*** Adoção de medidas para acessibilidade de participantes com necessidades especiais, levantamento de estatísticas sobre o público-alvo do evento.

Recomendações para proteção dos dados tratados:

- Os responsáveis devem providenciar comunicações claras e acessíveis sobre os objetivos dos eventos, incluindo a identificação de patrocinadores e parceiros envolvidos.
- Caso a divulgação dos eventos ocorra por listas de contatos já mantidas pelas entidades, oferecer opções de *opt-out* (descadastramento).
- A coleta de dados para organização de eventos deve se restringir aos dados essenciais para essa finalidade.
- Caso dados pessoais sensíveis sejam necessários, possibilitar que o titular não forneça tais informações e apresentar informações claras sobre a finalidade da coleta desses dados. Se possível, coletar o consentimento do titular.
- Selecionar empresas parceiras para organização do evento que cumpram com a LGPD.
- Quando da coleta de dados, forneça aos titulares informações claras e precisas sobre o exercício de seus direitos, como a eliminação de seus dados pessoais, se for o caso.

(ETAPA 2) DURANTE O EVENTO – INSCRIÇÃO E CREDENCIAMENTO

Exemplos de dados tratados e finalidades:

- **Dados cadastrais (nome completo, endereços de e-mail, números de telefone)**: credenciamento de participantes e palestrantes, controle de ingresso, realização de sorteios, inscrição em *newsletters* e outros materiais informativos.
- **Dados relativos à profissão, ao nível educacional, aos participantes com necessidades especiais e aos dados sobre raça e gênero:** análise do público-alvo.
- **Fotografias e filmagens:** registro dos participantes do evento, transmissão do evento *on-line* e gravação dos debates para registro futuro.

Recomendações para proteção dos dados tratados:

- Opções de *opt-in* e *opt-out* devem ser fornecidas, de forma clara, acessível e facilitada, para atividades, como a divulgação de próximos eventos, a exemplo do que ocorre por meio do envio de *e-mail marketing*, e/ou do envio de comunicados sobre os serviços prestados, mediante o envio de *e-mail marketing*.
- As informações sobre o uso dos dados pessoais durante os eventos devem estar acessíveis ao público.
- Os funcionários e colaboradores devem ser instruídos quanto ao atendimento de possíveis dúvidas sobre os titulares, fornecendo informações sobre o contato com o encarregado, por exemplo.
- Ao público geral podem ser fornecidos crachás de identificação que indiquem a sua preferência em não serem fotografados ou filmados.
- Durante o evento, caso sejam realizadas atividades audiovisuais (como a gravação e transmissão dos eventos on-lines, fotos e vídeos), é recomendável que essas práticas sejam amplamente informadas aos convidados, coletando o Termo de Autorização de Uso de Imagem sempre que necessário, com atenção especial aos casos que envolverem menores de idade.
- Quando da coleta de dados, forneça aos titulares informações claras e precisas sobre o exercício de seus direitos, como a eliminação de seus dados pessoais, se for o caso.

(ETAPA 3) APÓS O EVENTO – DIVULGAÇÃO DO EVENTO E DE AÇÕES DAS ENTIDADES DO SISTEMA INDÚSTRIA

Exemplos de dados tratados e finalidades:

- **Dados cadastrais (nome completo, endereços de e-mail, números de telefone)**: envio de materiais sobre o evento realizado, encaminhamento de convites para outros eventos similares –com mesmo público-alvo, compartilhamento de fotos e gravações, coleta de *feedbacks* e impressões.

Recomendações para proteção dos dados tratados:

- Os titulares podem ser informados previamente sobre as atividades relativas ao envio e processamento dos recibos de inscrição e certificados, com identificação das finalidades, dados pessoais envolvidos e o período de tempo pelo qual os dados serão tratados.
- Quando possível, os titulares devem ser informados previamente quanto aos registros de fotos institucionais a serem divulgadas e armazenadas em repositórios institucionais, coletando o Termo de Autorização de Uso de Imagem sempre que necessário, com atenção especial aos casos que envolverem menores de idade.
- Caso sejam coletadas informações de *feedbacks* e impressões sobre as atividades realizadas, recomenda-se a pseudonimização ou anonimização das informações, restringindo a vinculação direta das opiniões aos titulares.
- Forneça aos titulares informações claras e precisas sobre o exercício de seus direitos, como a eliminação de seus dados pessoais, se for o caso.
- Estabeleça protocolos de exclusão de dados após término do tratamento dos dados coletados nas fases anteriores.
- Caso tenham sido coletados dados para realização de estudos estatísticos, anonimizar as informações e descartar os dados pessoais desnecessários.

Assim, passa-se à análise das ferramentas e procedimentos que devem ser adequados para cada um dos momentos.

8.2 UTILIZAÇÃO DA PLATAFORMA CRM

Conforme mencionado no tópico anterior, o Sistema Indústria mantém base de dados com informações de parceiros institucionais que permitem o contato com esses titulares para divulgação de eventos. A principal ferramenta utilizada para essa finalidade é a ferramenta CRM, que permite o armazenamento de informações de contato de indivíduos que já participaram de algum evento promovido pelo Sistema Indústria ou já demonstraram interesse sobre determinados assuntos de eventos com participação das entidades desse sistema.

Por meio do sistema, é possível catalogar quais são os temas de interesse dos indivíduos catalogados. As categorias se relacionam com as temáticas dos eventos e as preferências são definidas a partir de participações anteriores do titular em outros eventos ou por meio da área de atuação do titular, a partir do seu papel profissional ou empresa que representa. Essas categorias são predeterminadas a partir das áreas de atuação e de realização de eventos pelo Sistema Indústria.

Com base nessa categorização, são formadas listas de interesse, para evitar que indivíduos recebam divulgações que fujam de sua expectativa para evitar o envio excessivo de material de divulgação.

Ressalta-se que, para garantir a autonomia do titular, este pode requerer a sua inclusão em outras listas, assim como a exclusão de suas informações – interrompendo o recebimento de materiais de divulgação.

Os dados, dessa forma, são obtidos de outro sistema de cadastro ou de documentação formulados após a realização de eventos. No âmbito nacional, as informações são acessadas pela área de eventos da CNI, dos Departamentos Nacionais do SENAI, e do SESI, bem como o Núcleo Central do IEL, que podem compartilhar essas informações com outros organizadores de eventos.

8.3 ATIVIDADES DE *MARKETING*

As técnicas de *marketing* ganharam novos contornos com os avanços de estratégias que otimizam o uso de dados pessoais para melhor alcance de seus objetivos, por meio da publicidade direcionada.

No âmbito de boas práticas internacionais de atividades de *marketing*, é possível indicar que o direcionamento de publicidade pode ocorrer por três principais formas:[104]

i) **direcionamento de publicidade com base em dados informados pelo próprio titular** (por ex. lista de *e-mails*);
ii) **direcionamento com base em dados coletados por conta da utilização de serviços ou aplicativos** (por ex. GPS, histórico de compras, etc.); e
iii) **direcionamento com base em dados inferidos** (por ex. formação de perfil por meio do comportamento em redes – histórico de navegação, "curtidas", etc.).

Nessa discussão, vale observar que a LGPD não proíbe a publicidade direcionada, mas acrescenta as condições de legitimidade para que os dados pessoais sejam utilizados, permitindo que instituições, como as que compõem o Sistema Indústria, se adequem à lei para aprimoramento dos resultados de suas ações.

Portanto, nos casos em que ocorrer direcionamentos com base em dados coletados e inferidos, é importante que se atente à forma do tratamento de dados. Isso porque, o uso dos dados do titular deve respeitar o princípio da não discriminação, não podendo

104 EDPB. **Guidelines 8/2020 on the targeting of social media users**. set. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf. Acesso em: 26 jun. 2023.

ser realizado tratamento para fins discriminatórios, ilícitos ou abusivos,[105] evitando-se, por exemplo, a configuração de ilícitos a partir do direcionamento de publicidade a partir de critérios manifestamente racistas, que violem o previsto na Lei nº 7.716/1989.[106]

No âmbito do Sistema Indústria, a utilização dos dados pessoais pode ocorrer, por exemplo, com apoio da Plataforma CRM para viabilização de campanhas de *e-mail marketing*, voltados à divulgação dos serviços desenvolvidos por si.

Quanto a este tema, é interessante citar o Código de Autorregulamentação para a Prática de *Email Marketing* (Capem) em 2009.[107] Desde esse período, algumas preocupações com o disparo de *e-mail*s já eram semelhantes às que temos hoje com a LGPD, sendo pontuados como aspectos centrais para o envio de *marketing* por *e-mail*:

Elementos centrais da utilização de bases de dados
(*art. 3º, CAPEM*)

- Identificação do remetente.
- Vedação da utilização de domínio de terceiro que não faça parte do grupo econômico do Remetente ou de parceiros.
- Indicação de assunto que seja relacionado ao conteúdo do *e-mail*.

Inclusão de opção de descadastramento (*opt-out*), com mais uma opção para contato para essa finalidade, além de inclusão de *link* que possibilite o descadastramento.

Padrões éticos para o envio de *e-mail*s para fins de publicidade
(*art. 4º, CAPEM*)

- Não é permitido o envio de *e-mail* para obtenção de permissão do destinatário para o envio de outros *e-mail*s.
- O envio de arquivos em anexo aos *e-mail*s deve ser precedido de autorização específica, prévia e comprovável do destinatário.
- Não é permitido enviar *link* que remeta a Códigos Maliciosos.[108]
- Não é permitida a utilização de recursos que disfarcem o código original da mensagem, devendo ser utilizado o formato.
- Imagens, áudios e vídeos devem ser hospedados em servidores pertencentes às empresas participantes do processo de envio do *e-mail marketing* ou contratadas pelas empresas.
- O remetente deve disponibilizar a política de *opt-out*, informando o prazo de remoção do seu endereço eletrônico da base de destinatários, não sendo obrigatório o seu uso na existência de contrato entre o remetente e o Destinatário (por exemplo, boleto bancário, avisos e extratos);
- O prazo para remoção de conteúdo não pode ser superior a 2 (dois) dias úteis, quando solicitado diretamente pelo *link* de descadastramento do *e-mail* for utilizado e 5 (cinco) dias úteis quando solicitado por outros meios.

105 SCHERTEL, Laura; FUJIMOTO, Mônica, MATTIUZZO, Marcela. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. *In*: DONEDA, Danilo *et al.* (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

106 Lei nº 7.716/1989. Define os crimes resultantes de preconceito de raça ou de cor.

107 O Código contou com a participação de grandes associações do mercado de anúncio e de comercio, a saber: ABA (Associação Brasileira de Anunciantes), Abemd (Associação Brasileira de *Marketing* Direto), Abradi (Associação Brasileira das Agências Digitais), Abranet (Associação Brasileira dos Provedores de Internet), Abrarec (Associação Brasileira das Relações Empresa Cliente), Agadi (Associação Gaúcha das Agências Digitais), Apadi (Associação Paulista das Agências Digitais), FecomércioRS (Federação do Comércio do Estado do Rio Grande do Sul), FecomércioSP (Federação do Comércio do Estado de São Paulo), Federasul (Federação das Associações Comerciais e de Serviços do Rio Grande do Sul), IAB (*Interactive Advertising Bureau do Brasil*), Internetsul (Associação dos Provedores de Acesso, Serviços e Informações da Rede Internet), Pro Teste (Associação Brasileira de Defesa do Consumidor), Seprorgs (Sindicato das Empresas de Informática do Rio Grande do Sul), tendo em vista a intenção da própria indústria em melhorar o uso do *email marketing*.

108 Art. 2º, IV, do Capem: Código Malicioso – Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms, bots*, cavalos de troia, *rootkits*, etc.).

Outra iniciativa autorregulada pertinente ao assunto se refere ao Código de Conduta para oferta de Serviços de Telecomunicações por meio de Telemarketing elaborado pelo Sistema de Autorregulação das Telecomunicações (SART). No código são apontadas como boas práticas na realização de ligações para consumidores:

Código de Conduta *Telemarketing* (SART)
(*art. 4º*)

- Não fazer ofertas sob pretexto de pesquisa ou sorteio, quando o verdadeiro objetivo for a comercialização de ofertas para os consumidores.
- Respeitar a vontade do consumidor sempre que ele manifestar a sua contrariedade quanto ao prosseguimento da ligação, encerrando a ligação e liberando a linha imediatamente.
- Não realizar ligações que não permitam a identificação pelos consumidores dos códigos de acesso utilizados pela prestadora na ligação.
- Não realizar ligações apenas para verificar a disponibilidade do consumidor em atender as ligações por meio de discador preditivo.
- Não finalizar as ligações abruptamente sem a identificação da prestadora e apresentação de ofertas.
- Realizar ligações apenas em horários oportunos compreendidos no período das 09 (nove) às 21 (vinte e uma) horas nos dias úteis e das 10 (dez) às 16 (dezesseis) horas nos sábados, salvo aquelas realizadas por solicitação ou com autorização dos consumidores, resguardadas as legislações específicas.
- Não realizar ligações nos domingos e feriados nacionais.
- Não realizar ligações de forma insistente, limitadas a no máximo 2 (duas) chamadas efetuadas pela empresa e recebidas pelo mesmo terminal de acesso do consumidor no mesmo dia, salvo aquelas realizadas por solicitação ou com autorização dos consumidores, resguardadas as legislações específicas.
- Não realizar ligações de forma insistente, limitadas a no máximo 15 (quinze) chamadas efetuadas pela empresa e recebidas pelo mesmo terminal de acesso do consumidor no mesmo mês, salvo aquelas realizadas por solicitação ou com autorização dos consumidores, resguardadas as legislações específicas.
- Não realizar ligações por meio de chamadas a cobrar para os consumidores;
- Não realizar ligações aleatórias ou para números sequenciais de consumidores.
- Assegurar que mensagens gravadas inseridas no início das ligações indiquem claramente a empresa que representa e informe o objetivo da ligação.

Tais recomendações possuem relação direta com o direito do consumidor,[109] sob a perspectiva da proteção de dados, uma vez que a utilização do *e-mail* ou do telefone para a oferta de produtos ou serviços também é considerada um tratamento de dados.

Além disso, os agentes de tratamento devem levar em consideração os direitos dos titulares e, especialmente, os princípios da finalidade, necessidade e transparência. Da mesma forma, é importante dispor de formas que garantam a transparência dos dados utilizados aos usuário, bem como estes devem ter acesso a meios claros e efetivos para realizar controle sobre suas informações.

109 "Art. 6º. São direitos básicos do consumidor: [...] IV – a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços".

Neste sentido, vale destacar que em outubro de 2022 a ANPD divulgou o "Guia Orientativo – *Cookies* e proteção de dados pessoais,"[110] que pretende estimular a "cultura da proteção de dados pessoais no ambiente digital, incentivando a adoção de práticas transparentes, que garantam maior compreensão e controle dos titulares sobre o uso de seus dados pessoais", nos termos da relatora do processo de elaboração deste documento, a Diretora Miriam Wimmer.

Entre as recomendações expostas no guia divulgado pela ANPD, é válido indicar que nos casos de adoção da base legal do consentimento para atividades de *marketing* por meio de *cookies*, seja ofertado ao titular a opção de *Gerenciamento de Cookies*. Com essa medida, é possível disponibilizar, de forma clara, acessível, gratuita e a qualquer momento, as opções de revisão de "permissões anteriormente concedidas" aos titulares.

O trabalho de tornar acessível aos titulares as informações sobre os motivos de coleta de seus dados, bem como ofertar disposições para exercício de seus direitos, exige dos profissionais responsáveis pelo *marketing* a exploração de medidas criativas para trazer ao seu público conteúdos sobre privacidade, em especial no meio digital.

Por isso, algumas medidas aconselhadas pelo "Guia GDPR para Profissionais de Marketing", desenvolvido pela WFA – *World Federation of Advertisers*,[111] podem ser consideradas como:

- Optar por disponibilizar informações acessíveis visualmente, com uso de ilustrações, símbolos e *emojis,* para explicar aos titulares as políticas de privacidade adotadas pela instituição.
- Priorizar textos curtos, simples e com o conteúdo relevante para cada hipótese, com a habilitação de atalhos para "Saiba mais", sempre que possível.
- Disponibilizar sistemas de uso fácil para deixar que os usuários controlem todas as configurações de privacidade em um único lugar, com a adoção de botões como "Eu me arrependo", para que o consentimento seja revisto pelo titular quando for desejado.
- Explicar aos usuários os motivos pelos quais os dados deles são necessários, com as justificativas sobre as consequências/implicações de dizer "sim" ou "não".

Dessa maneira, as práticas aqui recomendadas podem auxiliar as entidades do Sistema Indústria a desenvolver, manter e aprimorar melhores relações com seus parceiros, contando com a confiança dos titulares por meio das garantias de que a utilização dos dados cumpre com os fundamentos principiológicos da legislação.

110 BRASIL. Autoridade Nacional de Proteção de dados. **ANPD lança guia orientativo Cookies e Proteção de Dados Pessoais.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/anpd-lanca-guia-orientativo-201ccookies-e-protecao-de-dados-pessoais201d. Acesso em: 26 jun. 2023.

111 Orientações adaptadas a partir da ASSOCIAÇÃO BRASILEIRA DE ANUNCIANTES (ABA). **Guia GDPR para profissionais de Marketing**. 2020. Disponível em: https://aba.com.br/guia-gdpr-para-profissionais-de-marketing/. Acesso em: 26 jun. 2023.

Em relação às condições de legitimidade para o tratamento de dados, são basicamente duas as principais bases legais utilizadas para essa finalidade:[112] o consentimento – utilizado, quando aplicável, para *newsletters* divulgadas internamente – e o legítimo interesse – para envio de *e-mail marketing*, por exemplo. Essas duas bases legais são objeto de melhor atenção posteriormente neste Protocolo, no item VIII.5.

8.4 AGENTES DE TRATAMENTO ENVOLVIDOS

A organização de eventos requer alto investimento financeiro e pessoal. Além disso, é necessário envolver atores interessados no tema, inclusive para manter e otimizar relações com agentes relevantes para o desenvolvimento da indústria brasileira, colocando o Sistema Indústria e seus afiliados como protagonistas na discussão de diversos temas.

Para tanto, as entidades do Sistema Indústria mantêm relações com diversos parceiros, inclusive para realização de eventos institucionais. Dessa forma, existem duas principais situações em que as entidades do Sistema atuam na realização de eventos institucionais: (1) a entidade atua como única entidade organizadora do evento; ou (2) a entidade atua ao lado de parceiros para a realização do evento.

Em ambas as situações, as entidades do Sistema Indústria atuam como controladora de dados. Contudo, quando o evento é coorganizado em parceria com outras entidades, a entidade do Sistema Indústria atua como cocontrolador, em uma situação de controladoria conjunta.

Ressalta-se que em todos os casos, outras organizações poderão ser subcontratadas para auxílio na realização do evento. Nessa situação, as empresas terceirizadas atuam como operadoras de dados.

Além disso, para fins de controle do sucesso e relevância dos eventos e outras metas, informações pseudonimizadas sobre os participantes podem ser compartilhados com parceiros não organizadores, o que inclui patrocinadores.

8.5 CONDIÇÕES DE LEGITIMIDADE PARA O TRATAMENTO DE DADOS

Para a definição da base legal para o tratamento dessas informações, é importante ressaltar que esse tratamento não utiliza dados sensíveis. A própria finalidade do tratamento não justifica o tratamento de informações sensíveis, sendo tratados somente os dados estritamente necessários para esse fim: divulgação e realização de eventos institucionais.

112 EDPB. **Guidelines 8/2020 on the targeting of social media users**. set. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf. Acesso em: 26 jun. 2023. p. 14

Entende-se que nos três momentos assinalados, (pré, durante e pós-evento), a base legal mais apropriada para ser aplicada é a do legítimo interesse do controlador. Atividades, como envio de materiais para divulgação dos eventos, podem ocorrer pautadas na base legal do consentimento, como se verá adiante neste tópico.

O que se percebe desse contexto é que a utilização do consentimento como base legal requer avaliação cuidadosa, em especial sobre a possibilidade de garantir os direitos anteriormente indicados. Ainda assim, sua coleta não deve ser descartada, especialmente quando a base legal do legítimo interesse não for aplicável.

Em relação à aplicação dos princípios, a finalidade, adequação e necessidade possuem destaque, sendo necessário garantir que os dados coletados e utilizados serão proporcionais, adequados para a finalidade proposta e que o titular tenha a expectativa de que os seus dados serão utilizados para a finalidade que lhe foi informada.

Assim, ainda que exista a possibilidade de que os cadastros coletados no evento possam ser utilizados em cadastro para participar de um evento e os dados sejam utilizados posteriormente, com o intuito promocional, esta operação deve ser realizada com cautela, para que não seja excessivo. De preferência, sugere-se que o titular seja explicitamente informado sobre essa possibilidade quando do credenciamento no evento.

A coleta de dados deve se restringir apenas e tão somente ao necessário para o objetivo claro e específico exigido pelo tratamento em questão. Atenção especial deve ser dispensada para que o tratamento de dados realizado não tenha o potencial de prejudicar os direitos dos titulares ou possa exceder as suas legítimas expectativas, especialmente se utilizada a base legal do legítimo interesse.

8.5.1 CONSENTIMENTO

De início, vale pontuar que a base legal do consentimento exige uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII, da LGPD).

Conforme observado pela Autoridade do Reino Unido, a *Information Commissioner's Office* (ICO), a coleta do consentimento deve ser acompanhada das opções de *opt-out* e o *opt-in*, sendo necessária a identificação da finalidade específica do tratamento. Por isso, percebe-se que a coleta do consentimento como base legal para publicidade (em especial a digital) pode comprometer o alcance da estratégia, além de ser capaz de estar restrita a um público que já teve contato com a marca/empresa, além de levantar dificuldades

sobre "o bombardeio de pessoas com solicitações de consentimento desnecessárias e a '*consent fatigue*.'"[113]

A expressão fadiga de cliques também é utilizada pelo *European Data Protection Board* (EDPB), para demonstrar as centenas de pedidos de consentimento que o titular encontra diariamente, que ressalta o risco de que se reduza os efeitos do consentimento como um instrumento de aviso e de reflexão do titular.[114]

É nesse sentido que alguns requisitos devem ser observados quando se decidir sobre o uso do consentimento para fins de *marketing*:

- oferecer uma escolha real, devendo constar de cláusula destacada das demais cláusulas contratuais caso seja fornecido por escrito (art. 8º, § 1º), LGPD);
- possibilitar que o titular possa retirar o consentimento quando bem entender (caso não seja possível, o consentimento não é a base legal adequada (art. 8º, § 5º);
- controlador deve comprovar que o consentimento foi obtido de forma adequada (art. 8º, § 2º);
- ser fornecido para finalidades determinadas, não sendo permitida a utilização de autorizações genéricas (art. 8º, § 4º);
- caso o controlador necessite compartilhar os dados com outros controladores, é necessária a coleta de consentimento específico para este fim; e
- garantir que o titular possa receber cópia integral de seus dados pessoais em formato que permita sua utilização subsequente, nos termos a serem regulamentados pela ANPD e respeitados os segredos comercial e industrial (art. 19, § 3º).

A coleta do consentimento pode ser realizada de diversas formas como formas de cumprir as disposições da LGPD. Exemplos comuns, que podem continuar sendo utilizados pelo Sistema Indústria ou implementados, caso ainda não ocorram, são: instrumentos contratuais, formulários, cadastros realizados para utilização de plataforma digital ou *site*, aviso de *cookies*. A respeito destes, o seu uso não é obrigatório no Brasil, diferente do que ocorre na Europa, que possui legislação específica sobre o tema.[115]

Ainda assim, a utilização de caixas (ou *banner* de *cookies*) é recomendada para os casos nos quais o consentimento pode ser coletado – em especial quando forem coletados *cookies* que não são estritamente necessários – e para que o(a) usuário(a) seja direcionado para a central de gerenciamento de opções.

113 INFORMATION COMISSIONER'S OFFICE – ICO. **When can we rely on legitimate interests?** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/. Acesso em: 26 jun. 2023.

114 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 05/2020 on consent under Regulation 2016/679**. maio 2020. p. 19. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 22 jun. 2023.

115 EUROPEAN UNION. DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009. amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. **Official Journal of the European Union**, l337/11, 18 dez. 2009. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF. Acesso em: 26 jun. 2023.

No mais, as caixas de aviso podem ser uma importante fonte de informações a respeito das finalidades dos *cookies* utilizados, em atenção aos princípios da boa-fé e transparência com a coleta de dados. Logo, antes da coleta ser realizada, em todas as etapas em que ela for feita deve-se exibir claramente o propósito deste tratamento.

Na hipótese de o consentimento ser obtido por caixas de confirmação, é recomendável que essas apresentem devidamente a descrição da finalidade específica e não estejam pré-preenchidas quando o usuário for realizar algum cadastro, com manifestas especificações sobre como os *cookies* funcionam, para o quê os dados de *cookies* serão usados e por quanto tempo serão retidos.

Nesse sentido, também é interessante incluir a descrição das categorias de *cookies* conforme seus respectivos usos e finalidade. No caso dos *cookies* não necessários,[116] não é recomendável que eles sejam apresentados aos titulares como aceite padrão e se exija a desativação manual pelo titular.[117]

A ANPD[118] recomenda que seja elaborada uma política de *cookies* que disponibilize informações sobre as finalidades específicas que justificam a sua coleta, período de retenção das informações e hipóteses de compartilhamento com terceiros. Tal política pode ser apresentada das seguintes formas: i) como uma seção específica do Aviso de Privacidade; (ii) em um local específico e separado; ou (iii) no próprio banner de *cookies*.

De acordo com a *ePrivacy Directive* da União Europeia, Diretiva 2009/136/EC, o armazenamento de informações coletadas por meio de *cookies* (considerando 66) deve ser acompanhada por informações claras e concisas e devem permitir a revisa ou solicitar o consentimento do usuário. Esse procedimento apenas é dispensado quando os *cookies* são estritamente necessários. Para tanto, recomenda-se que não sejam utilizadas frases complexas e jargões, para garantir que os usuários efetivamente tenham informações sobre o fornecimento do seu consentimento para a coleta de dados, com exceção dos *cookies* estritamente necessários.[119] Ademais, todo o consentimento do usuário deve ser documentado e armazenado pela instituição.

116 Para maiores explicações sobre as categorias dos *cookies*, consulte: BRASIL. Autoridade Nacional de Proteção de Dados – ANPD. **Guia Cookies e proteção de dados pessoais**. Brasília: 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 26 jun. 2023.

117 BRASIL. Autoridade Nacional de Proteção de Dados – ANPD. **Guia Cookies e proteção de dados pessoais**. Brasília: 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 26 jun. 2023.

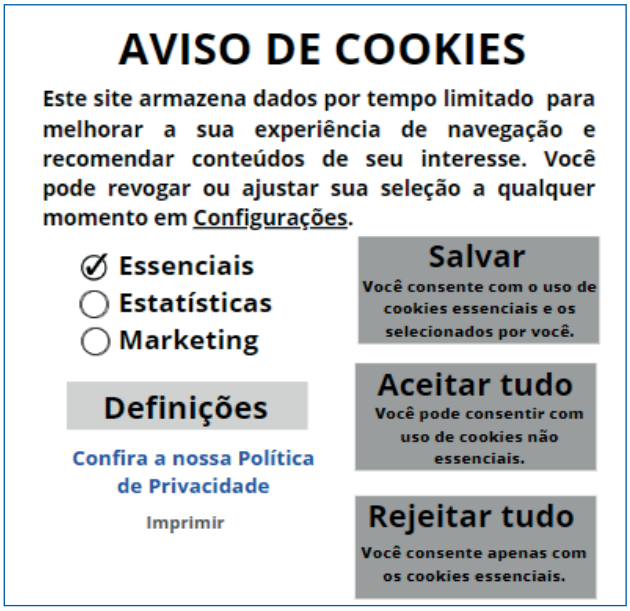
118 BRASIL. Autoridade Nacional de Proteção de Dados – ANPD. **Guia Cookies e proteção de dados pessoais**. Brasília: 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 26 jun. 2023.

119 GDPR.EU. **Cookies, the GDPR, and the ePrivacy Directive**. 2023. Disponível em: https://gdpr.eu/cookies. Acesso em: 26 jun. 2023.

O acesso ao *site* não deve ser inviabilizado caso o consentimento sobre o uso de *cookies* não seja fornecido, bem como tenham a capacidade de retirar o consentimento do uso de *cookies* sem dificuldades. Caso o *cookie* ou rastreador não possam ser desabilitados por meio do navegador, o titular também deve ser informado sobre este procedimento.[120]

A seguir, apresentamos um modelo de *banner* de *cookies* com a opção de "recusa" e um modelo de *banner* com a opção de "consentimento" que pode ser utilizado como exemplo:

Modelo de *banner* de *cookies* com a opção de "recusa".



Modelo de *banner* de *cookies* com a opção de "consentimento".

120 BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia Cookies e proteção de dados pessoais**. Brasília: 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 26 jun. 2023.

Para a atividade de realização de eventos institucionais, também pode ser coletado o consentimento dos titulares para solicitar autorização para envio de materiais de divulgação e, em especial, para a utilização da imagem do titular. No caso da utilização da imagem, pode ser coletado o consentimento por meio de contrato específico celebrado para essa finalidade, o "Termo de Uso de Imagem". Nesse caso, a base legal aplicável seria a execução de contrato, devendo ser obedecido o previsto no art. 20 do Código Civil.[121]

Importante considerar que o consentimento deve ser utilizado apenas quando o tratamento apresentado não oferecer riscos relevantes aos direitos e liberdades fundamentais ao titular, devendo ser garantido ao indivíduo a possibilidade de optar por interromper o recebimento dos materiais de divulgação.

Ainda sobre o uso da imagem, em fotos, vídeos ou outros meios possíveis, é importante considerar que as imagens coletadas não podem ser utilizadas fora do contexto pelo qual essa coleta foi justificada, pois qualquer "uso descontextualizado implicará em violação à finalidade do consentimento obtido."[122]

Em caso de campanhas que queiram vincular a imagem dos usuários de serviços e atividades prestadas pelas entidades e órgãos do Sistema Indústria, por exemplo, é importante que também sejam compartilhadas aos titulares o objetivo da campanha e escopo de divulgação, isto é, se as imagens serão divulgadas em redes sociais ou cartazes.[123]

Logo, a utilização dessa base deve garantir que o consentimento coletado seja "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII, da LGPD*)*. Para garantir que a manifestação seja informada, o EDPB recomenda que algumas informações sejam apresentadas:[124]

- Identidade do controlador.
- Finalidade das operações de tratamento para as quais o consentimento é solicitado.
- Tipo de dado que será coletado e tratado.
- Informações sobre a retirada do consentimento.
- Informações sobre a tomada de decisões automatizadas.

121 Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

122 FUNDAÇÃO GETULIO VARGAS – FGV. **Guia de proteção de dados pessoais:** *marketing*. out. 2020. p. 40. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_marketing.pdf. Acesso em: 26 jun. 2023.

123 FUNDAÇÃO GETULIO VARGAS – FGV. **Guia de proteção de dados pessoais:** *marketing*. out. 2020. p. 40. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_marketing.pdf. Acesso em: 26 jun. 2023.

124 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 05/2020 on consent under Regulation 2016/679**. maio 2020. p. 15. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 22 jun. 2023.

Dessa maneira, entende-se que o uso do consentimento pode ser interessante em casos nos quais as tecnologias utilizadas para o direcionamento das atividades de *marketing* utilizem dados inferidos ou possam ser considerados excessivos, como a localização geográfica do titular.

De acordo com o que será apresentado no próximo item, identifica-se que o uso da base legal do legítimo interesse não comporta o tratamento de dados capazes de prejudicar os direitos dos titulares ou que possa exceder as suas legítimas expectativas.[125] Por isso, quando houver dúvidas sobre a aplicação do legítimo interesse, o consentimento também se mostra como uma base legal recomendável.

8.5.2 LEGÍTIMO INTERESSE

Em razão das dificuldades apresentadas pelo uso do consentimento, observa-se na prática a ampla utilização do legítimo interesse para fins de *marketing*.

Autoridades como a *Information Commissioner's Office* (ICO) recomendam a utilização dessa base legal, prevista no art. 7º, IX, da LGPD, por ser mais simples em relação à base legal do consentimento. Esse fato acontece a partir da divulgação de fácil acesso e compreensão sobre o tratamento de dados realizado ao titular, bem como de previsão para que estes possam excluir seus dados para tal finalidade.[126] Dessa forma, compreende-se que a base do legítimo interesse pode trazer vantagens para o tratamento, uma vez que o consentimento pode não ser facilmente coletado ou pode não ser passível de revogação.

Ressalta-se que a ANPD[127] já se posicionou sobre a impossibilidade de utilização do legítimo interesse nos casos em que dados coletados por meio de *cookies* são utilizados para publicidade, especialmente se ocorre a coleta de *cookies* de terceiros. Assim, a autoridade entende que o consentimento é a base legal mais apropriada para essa finalidade, especialmente por conta do risco de formação de perfis comportamentais, análise e previsão de preferências, além da possibilidade de rastreamento do usuário. Para os outros casos que não envolvem a coleta de *cookies*, o legítimo interesse pode ser considerado uma base legal adequada.

125 EDPB. **Guidelines 8/2020 on the targeting of social media users**. set. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf. Acesso em: 26 jun. 2023.

126 INFORMATION COMISSIONER'S OFFICE – ICO. **When can we rely on legitimate interests?** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/. Acesso em: 26 jun. 2023.

127 BRASIL. Autoridade Nacional de Proteção de Dados – ANPD. **Guia Cookies e proteção de dados pessoais**. Brasília: 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 26 jun. 2023.

De acordo com o Código de Conduta do setor publicitário espanhol, caso se opte pela escolha desta base, é preciso considerar:[128]

i) as expectativas dos titulares;
ii) se os titulares são grupos minoritários ou que necessitam de proteção adicional por conta de alguma vulnerabilidade;
iii) se o titular pode se opor ao tratamento com facilidade;
iv) se a publicidade se baseia na formação de perfis; e
v) frequência dos envios.

É por isso que a confecção da Avaliação de Legítimo Interesse (*Legitimate Interests Assessment* – LIA) pode ser adotada no processo de tomada de decisão sobre a aplicação desta base legal, uma vez que ela é considerada mais ampla em relação às demais. Em acréscimo, é recomendável que esta medida ocorra antes que o tratamento seja iniciado ou quando a finalidade do tratamento foi modificada.

Da mesma forma, a LGPD estipula que se pode usar o legítimo interesse para "apoio e promoção de atividades do controlador" (art. 10, I, da LGPD); e "proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem" (art. 10, II, da LGPD).

Nesse sentido, cabe ao controlador observar alguns parâmetros, como:

- respeitar as expectativas dos titulares (art. 10, II, da LGPD);
- respeitar os direitos e liberdades fundamentais dos titulares (art. 10, II, da LGPD);
- utilizar apenas dados estritamente necessários para a finalidade pretendida (art. 10, § 1º, da LGPD);
- adotar medidas que garantam a transparência no tratamento de dados (art. 10, § 2º, da LGPD); e
- apresentar relatório de impacto à ANPD quando ela solicitar (art. 10, § 3º, da LGPD).

Do analisado, pode-se concluir que o legítimo interesse não deve ser considerado o "último recurso" quando dados não sensíveis forem tratados, pois o seu uso pode gerar grande insegurança aos titulares, implicando em maior atenção aos agentes de tratamento.

128 AGENCY SPANISH PROTECTION DATA – AEPD. **Resolution approving the code of conduct and accreditation of the monitoring body**. Cc/0004/2018 2018. Disponível em: https://edpb.europa.eu/sites/default/files/conduct/resolucion-aprobacion-cc.0004.2018-autocontrol_en.pdf. Acesso em: 26 jun. 2023.

Em atenção às melhores práticas internacionais,[129] sugere-se que, os seguintes elementos sejam observados quando no período de confecção do LIA:

- Contexto, propósito e benefício das atividades de processamento de dados, além dos riscos de não realizar o processamento.
- O interesse legítimo do controlador, terceiros ou grupos de indivíduos ou da sociedade, assim como seus direitos e liberdades e outros direitos relativos à proteção de dados.
- Interesses, liberdades e direitos dos titulares, bem como suas expectativas legítimas nas quais estão fundadas a sua relação com o controlador.
- Riscos e danos que podem resultar do tratamento ou da ausência de tratamento, bem como a gravidade que tais danos podem causar aos titulares.

Para análise desses elementos, recomenda-se a utilização do teste de 3 (três) etapas, para que seja verificado**: i) a finalidade, ii) a necessidade e iii) a proporcionalidade.**[130]

PARTE 1 – Identificando o legítimo interesse

Qual o propósito do processamento de dados?
Qual o benefício que se espera do processamento?
O tratamento de dados pessoais é realizado pelo controlador ou por terceiro para atender um legítimo interesse da Companhia?
Por que esse processamento é importante para o controlador?
Algum interesse público pode ser atingido com o processamento?
Existe algum problema ético ou discriminatório no processamento?

PARTE 2 – Teste da necessidade

Este processamento irá auxiliar no propósito buscado?
Este propósito pode ser atingido de outras formas?
É possível atingir o mesmo objetivo utilizando menos dados ou processando esses dados de forma menos invasiva?

129 INFORMATION COMISSIONER'S OFFICE (ICO). **How do we apply legitimate interests in practice?** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/. Acesso em: 26 jun. 2023; CIPL. **How the "legitimate interests" ground for processing enables responsible data use and innovation**. 2021. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf. Acesso em: 26 jun. 2023; IAPP. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. 2018. Disponível em: https://iapp.org/resources/article/guidance-on-the-use-of-legitimate-interests-under-the-eu-general-data-protection-regulation/. Acesso em: 26 jun. 2023.

130 CONEXIS. **Código de boas práticas de proteção de dados para o setor de telecomunicações**. Disponível em: https://conexis.org.br/setor-de-telecomunicacao-publica-codigo-de-boas-praticas-para-a-protecao-de-dados/. Acesso em: 22 jun. 2023.

PARTE 3 – Teste da proporcionalidade

Há expectativa do titular de que esses dados sejam tratados?
Qual a natureza da relação entre o titular dos dados e o controlador?
Quais os possíveis impactos do tratamento de dados nos titulares e o quão graves eles podem ser?
Algum dos titulares vulneráveis de alguma forma?
Os dados foram obtidos diretamente dos titulares?
É possível oferecer o *opt-out* ao titular sem que o tratamento seja comprometido?
Informações sobre o tratamento de dados são fornecidas ao titular? A comunicação clara e anterior aos propósitos do tratamento de dados?
É possível adotar salvaguardas?

Vale frisar que o teste anteriormente indicado não pretende apresentar alguma resposta exata sobre a possibilidade de utilização desta base legal, uma vez que é necessária a avaliação do controlador se os benefícios gerados pelo processamento não serão superados pelos riscos.

Por fim, caso ainda não tenham sido adotadas, é recomendável a adoção de salvaguardas e controles, sempre que possível, a exemplo de medidas de anonimização, controle de acesso aos dados, mecanismos de autenticação, inventário com acessos aos registros de conexão e acesso a aplicações.

9 PROTOCOLO PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS

9.1 INTRODUÇÃO

A transferência internacional de dados é uma das formas de tratamento de dados pessoais pela qual ocorre a transferência dos dados para país estrangeiro ou organismo internacional do qual o país seja membro. Entre as atividades de tratamento de dados desempenhadas pelas entidades do Sistema Indústria, ressalta-se que a contratação de serviços de hospedagem e a relação com organismos internacionais e entidades congêneres são as principais que exigem esse tipo de transferência.

Para que seja possível esse compartilhamento internacional, a LGPD estabelece que os países ou organismos internacionais dos quais o país seja membro que irão receber os dados apresentem grau de proteção de dados pessoais adequado, conforme avaliação da ANPD. Essa avaliação envolve a observância dos princípios e direitos dos titulares da LGPD, a natureza dos dados, as normas gerais e setoriais da legislação em vigor no local de destino, e a adoção de medidas de segurança previstas em regulamento, por exemplo.

O art. 33 da LGPD define três regimes[131] de tutela dos dados quando da transferência internacional de dados: (i) declaração de existência de grau de proteção adequado; (ii) existência de garantias de cumprimento com os preceitos da lei; e (iii) derrogações específicas que tem como objetivo a promoção de interesse público.

A partir desses três regimes, a LGPD estabelece em seu art. 33 os seguintes instrumentos legais que legitimam a transferência internacional de dados:

131 PRATA DE CARVALHO, Angelo. Transferência internacional de dados na lei geral de proteção de dados: força normativa e efetividade diante do cenário transnacional. *In*: TEPEDINO, Gustavo *et al.* (Coords.). **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 624.

Países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado (inciso I)	• O nível de proteção do país necessita de análise pela ANPD. • A decisão de adequação será pautada nos seguintes critérios: I – as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; II – a natureza dos dados; III – a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; IV – a adoção de medidas de segurança previstas em regulamento; V – a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e VI – outras circunstâncias específicas relativas à transferência.
Garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD (inciso II)	• A transferência internacional pode ocorrer quando o controlador garantir o cumprimento do regime de proteção de dados da LGPD, por meio de: a) cláusulas contratuais específicas; b) cláusulas contratuais padrão; c) normas corporativas globais; e d) selos, certificados e códigos de conduta.
Cooperação jurídica internacional entre órgãos públicos de inteligência (inciso III)	• Não se aplica a agentes privados. • A transferência pode ocorrer caso existam acordos bilaterais entre órgãos públicos.
Proteção da vida ou da incolumidade física do titular ou de terceiros (inciso IV)	• Hipótese excepcional deve ser utilizada apenas quando a vida do titular ou do terceiro dependa do tratamento de dados possibilitado pela transferência internacional. • Não é possível realizar interpretação ampla sobre proteção da vida, assim como na aplicação do art. 7º, VII, e 11, II, "e", da LGPD.
Autorização pela ANPD (inciso V)	• Hipótese ampla que possibilita que transferências internacionais sejam realizadas quando a ANPD autorizar, possibilitando que a Autoridade avalie as especificidades de cada caso.
Compromisso assumido em acordo de cooperação internacional (inciso VI)	• Hipótese garante que os instrumentos de cooperação não sejam submetidos a procedimentos excessivamente burocráticos que podem comprometer relações diplomáticas.
Execução de política pública (inciso V)	• Não se aplica a agentes privados. • Hipótese deve ser utilizada pelos agentes que possuem prerrogativas para tanto, não sendo necessária a sua submissão à ANPD.
Consentimento (inciso VIII)	• Para ser válido, deve ser livre, informado e inequívoco; além de cumprir com os requisitos de transparência e acesso à informação. • O titular deve ser informado de forma específica sobre essa modalidade de tratamento. • Importa notar que nem sempre o consentimento será a base mais adequada, tendo em vista as restrições mencionadas na Parte I.
Hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD (inciso IX)	Possibilita a utilização de bases legais que já permitem a realização de tratamento de dados em território nacional, quais sejam: i) cumprimento de obrigação legal ou regulatória (art. 7º, II, da LGPD); ii) execução de contrato do qual o titular seja parte (art. 7º, V, da LGPD); e iii) exercício regular de direitos (art. 7º, VI, da LGPD).

Insta ressaltar, contudo, que a ANPD ainda deve se manifestar sobre questões centrais para a correta utilização das bases legais anteriormente indicadas. Entre os temas, pode-se depreender do texto do art. 35 da LGPD que caberá à Autoridade Nacional "a *definição do conteúdo* de cláusulas-padrão contratuais, bem como a *verificação* de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta" (grifo nosso).

Ainda assim, serão apresentadas algumas diretrizes gerais sobre as duas principais formas de compartilhamento internacional de dados identificadas no Sistema Indústria, a saber, a contratação de serviços de hospedagem e a relação com entidades congêneres.

9.2 CONTRATAÇÃO DE SERVIÇOS DE HOSPEDAGEM

Os serviços de hospedagens referem-se aos locais nos quais os dados são armazenados, incluindo a disponibilização de *hardware*, sistemas, *softwares* e infraestrutura necessária para manutenção dos dados, gerenciamento de acesso aos dados e atividades relacionadas, como a garantia de qualquer processo voltado à recuperação e acesso à base de dados após eventuais incidentes.[132] Vale indicar que a hospedagem pode ser feita por diferentes formas se os dados estiverem disponíveis na internet e acessíveis para este fim, o que requer a disponibilização de sistemas e acesso a outros serviços disponíveis na internet.

Entre as principais modalidades, estão os bancos de dados e a hospedagem de *sites*, arquivos ou domínio da *web*. Então, por exemplo, se esses bancos de dados estiverem localizados fora do território brasileiro, trata-se de hipótese de transferência internacional de dados. Para identificação da legislação aplicável e se a operação configura transferência internacional de dados, as entidades devem observar o país no qual o servidor está localizado, uma vez que a LGPD dispõe que quaisquer transferências de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro, configurará uma transferência internacional de dados (art. 5º, XV, da LGPD).

Os serviços de armazenamento em *cloud* (ou nuvem) possibilitam que aquele que hospeda o Sistema Indústria tenha acesso aos dados armazenados por si, por meio do uso do serviço contratado. No âmbito nacional, o Sistema Indústria utiliza diferentes plataformas que se enquadram nesta categoria, como o Microsoft Azure, Microsoft 365, Oracle Cloud e Amazon AWS.

132 LAW INSIDER. **Data Hosting Services definition**. Disponível em: https://www.lawinsider.com/dictionary/data-hosting-services; COMISSÃO EUROPEIA. **Registo INSPIRE:** data processing, hosting and related activities. Disponível em: https://inspire.ec.europa.eu/codelist/EconomicActivityNACEValue/J.63.11. Acesso em: 26 jun. 2023.

Ainda que, atualmente, o tema esteja pendente de regulamentação pela ANPD, é possível adotar medidas de segurança para prevenir incidentes de segurança. É importante que sejam garantidas medidas técnicas de segurança dos dados, para reduzir as chances de acesso, alteração, exclusão ou compartilhamento dos dados de forma indevida. Ademais, deve-se considerar os princípios previstos na LGPD, em especial o da necessidade, finalidade e adequação.

Também é recomendado que as empresas de hospedagem garantam a proteção dos dados, o que pode ser observado não apenas por meio dos contratos firmados, como por meio da elaboração do Acordo de Processamento de Dados, conforme exposto no Protocolo VI, para a elaboração de acordos entre agentes de tratamento, supra. Nessas oportunidades, deve-se prezar pela clareza na compreensão dos métodos utilizados para o tratamento dos dados, garantindo-se, por exemplo, a tradução dos documentos com empresas firmadas caso existam em idiomas diferentes do português.

Ademais, o processo de contratação da empresa de hospedagem deve considerar as medidas de segurança da informação adotadas, histórico de incidentes de segurança, adequação com o previsto na LGPD, entre outros. Após a contratação das empresas também se deve acompanhar as alterações nas políticas de privacidade e eventuais incidentes de segurança que ocorram para que a manutenção do contrato seja avaliada periodicamente. Em caso de contratos de longo prazo, incidentes de segurança podem ser incluídos como hipóteses para rescisão contratual por justa causa.

9.3 RELAÇÃO COM ENTIDADES CONGÊNERES

As entidades congêneres são as instituições que desempenham as funções semelhantes da CNI em outros países. Esta relação é fundamental para aperfeiçoamento dos produtos internos e parcerias comerciais, de modo que estes estejam de acordo com as melhores práticas internacionais.

Em anos anteriores, a CNI firmou parceria com a Câmara de Comércio dos Estados Unidos, que representa mais de 3 milhões de empresas deste país,[133] criou o Fórum de Executivos Brasil-Índia,[134] além de estabelecer acordo para crescimento do comércio entre o país e a Holanda.[135]

133 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **CNI firma parceria sobre propriedade intelectual com congênere americana**. 2014. Disponível em: https://noticias.portaldaindustria.com.br/noticias/inovacao-e-tecnologia/cni-firma-parceria-sobre-propriedade-intelectual-com-congenere-americana/. Acesso em: 26 jun. 2023.

134 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **CNI e congênere indiana criam Fórum de Executivos Brasil-Índia**. Disponível em: https://noticias.portaldaindustria.com.br/noticias/economia/cni-e-congenere-indiana-criam-forum-de-executivos-brasil-india/. Acesso em: 26 jun. 2023.

135 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **CNI e congênere holandesa assinam acordo para elevar comércio entre Brasil e Holanda**. Disponível em: https://noticias.portaldaindustria.com.br/noticias/internacional/cni-e-congenere-holandesa-assinam-acordo-para-elevar-comercio-entre-brasil-e-holanda/. Acesso em: 26 jun. 2023.

Esse protagonismo da CNI pode ser aprimorado com a proposição de modelos de contratos ou instrumentos de parceria que contenham previsões expressas sobre quais os dados devem ser transferidos, quais as finalidades e quem são os agentes que os receberão. Ademais, também é possível realizar uma análise profunda sobre a necessidade de compartilhamento de dados pessoais na execução dos acordos com as referidas entidades.

Neste sentido, é sugerido o acompanhamento das regulamentações futuras da ANPD e das disposições das autoridades de proteção estrangeiras nas quais estão localizados os dados, com maneira de resguardar a integridade e segurança nessa modalidade de compartilhamento.

PARTE 3

PROTOCOLOS ESPECÍFICOS

1 CNI

1.1 INTRODUÇÃO

A CNI possui o propósito de representar e coordenar ações e estudos de interesses das categorias econômicas do setor industrial. Assim, atua "na defesa e na promoção de políticas públicas que favoreçam o empreendedorismo e a produção industrial, num setor que reúne mais de 476 mil indústrias no país."[136]

Em acréscimo, as federações de indústrias estão presentes nos 26 estados e Distrito Federal, atuando na defesa e representação das indústrias locais perante os governos estaduais e municipais. Por meio delas, há a conexão desses atores locais com a CNI, que ocorre por meio do fornecimento de informações gerais sobre o panorama geral da indústria, bem como auxiliando no desenvolvimento de projetos específicos.

A CNI possui papel central de diálogo entre o setor da indústria e demais agentes econômicos e políticos. A atenção com as mudanças legislativas, por exemplo, a motivou a participar ativamente do processo de construção da LGPD e a incluir a necessidade de uma lei sobre dados pessoais na Pauta Mínima da Agenda Legislativa da Indústria.[137]

Ainda assim, existem algumas especificidades no tratamento de dados de cada uma das entidades, motivo pelo qual destacaremos as particularidades das principais operações de tratamento de dados de cada entidade nesta Parte III. Avaliaremos os tipos de dados tratados, assim como as suas finalidades, bases legais aplicáveis e medidas procedimentais que podem ser adotadas para redução dos riscos envolvidos nas operações de tratamento.

Nesse sentido, uma das suas principais frentes de atuação consiste no diálogo e articulação com o poder público e outras entidades por meio de seus diversos órgãos. O Fórum Nacional da Indústria (FNI), por exemplo, conta com dezenas de líderes empresariais e entidades que são responsáveis por desenvolver estratégias para a indústria. Já os Conselhos Temáticos Permanentes consistem em outra iniciativa central que envolve representantes das federações estaduais, associações setoriais e empresas industriais, e possuem importante

136 CONFDEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Áreas de atuação**. Disponível em: https://www.portaldaindustria.com.br/cni/institucional/.

137 CONFDEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **LGPD**: o que a sua empresa precisa saber. Brasília: CNI, 2020. p. 7. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/d6/29/d6297686-923a-4f69-8d4b-ff81bb4e8eb8/lgpd_o_que_sua_empresa_precisa_saber.pdf. Acesso em: 26 jun. 2023.

função na atualização constante dos membros com informações e propostas sobre temas diversos que permeiam os interesses da indústria.

Há ainda outra forma de atuação, que envolve a representação da indústria em colegiados que debatem políticas públicas em diversas áreas com impacto sobre a atividade industrial. Esse fato se deve à existência no Governo Federal de diversas instâncias de representação, que contam com a participação de representantes da indústria.

A interlocução entre os poderes é essencial para garantir que os objetivos da CNI sejam alcançados, em especial, a defesa e promoção de políticas públicas que favoreçam o empreendedorismo e a produção industrial.

Tais atividades exigem diferentes formas de relacionamento que ocorrem a partir do tratamento de dados pessoais, quais sejam:

- Contato direto com as Autoridades Públicas e Setor Privado.
- Elaboração de perfis de tomadores de decisão (autoridades e parlamentares), interessados e influenciadores.
- Ações Preparatórias (reuniões técnicas; elaboração de notas técnicas e sugestões de textos legislativos; redação de parecer; análise de votação, etc.).
- Acompanhamento de ações governamentais com impacto setorial e institucional (Executivo, Legislativo e Judiciário).
- Exercício de direitos em processos administrativos e judiciais.
- Monitoramento e participação em grupos de representação perante o Poder Público.
- Promoção de Eventos Institucionais para gerar aproximação entre o Sistema Indústria e Setores Público, Privado e Sociedade.

A partir dessas estratégias, identificamos duas importantes atividades que envolvem operações de tratamento de dados da CNI: tratamento de dados para fins de relações governamentais e exercício de direitos em processos administrativos ou judiciais. Assim, passa-se à análise dessas duas atividades.

1.2 TRATAMENTO DE DADOS PARA FINS DE RELAÇÕES GOVERNAMENTAIS

Em razão de a CNI ser alcançada por diferentes temas, o acompanhamento das atividades públicas exige comumente uma ação coordenada com os agentes públicos, com o intuito de garantir a iniciativa sobre determinado tema ou para apresentação dos posicionamentos da indústria sobre uma temática.

Por isso, a apresentação de temas e posicionamentos de interesse da indústria é uma das formas de atuar em parceria com autoridades e garantir a exploração de temas de relevância para a indústria. Assim, a CNI pode levar a uma Autoridade pleitos do setor industrial por meio de reuniões técnicas ou por meios de comunicação como *e-mails*, aplicativos de mensageria, entrega de memoriais, entre outros.

As ações de influência podem incentivar o início do debate sobre determinado assunto, e garantir que autoridades parceiras levem os interesses da indústria para o pleito.

Dessa forma, para garantir que todas as pautas de interesse da indústria sejam acompanhadas, as demandas podem ser encaminhadas a unidade(s) responsável(eis) pelo relacionamento com o Poder Executivo – que acompanham a agenda pública das autoridades, principalmente os membros do Poder Executivo. As agendas são acompanhadas por meio dos *sites* públicos, bem como por meio do contato direto com a autoridade ou assessoria. Esse diálogo direto é feito por diversos meios, como ligações telefônicas, envio de mensagens privadas ou *e-mail*.

Dessa forma, considerando todas essas finalidades, a(s) unidade(s) pode(m) criar um **perfil da Autoridade**. Esse perfil deve ser cadastrado na ferramenta CRM e contará com informações das mais diferentes fontes. O perfil registra dados extraídos de fontes diversas, posicionamentos prévios das autoridades sobre determinados temas, quais temáticas contam com a atuação daquela autoridade e qual a prioridade do tema para o agente público. Logo, é relevante considerar que diversos tipos de dados são tratados com o objetivo de manter ou construir relações com autoridades.

Os dados públicos são também conhecidos como dados abertos. Segundo definição da *Open Knowledge Foundation*,[138] "dados são abertos quando qualquer pessoa pode livremente acessá-los, utilizá-los, modificá-los e compartilhá-los para qualquer finalidade, estando sujeito a, no máximo, exigências que visem preservar sua proveniência e sua abertura."

O Poder Executivo Federal conta com uma política de dados abertos,[139] determinando a publicação de diversas informações. Além disso, vários setores – inclusive o Sistema Indústria – são afetados e devem observar regras da Lei de Acesso à Informação (LAI – Lei nº 12.527/11).

138 JAMES, Laura. **Defining Open Data**. out. 2013. Disponível em: https://blog.okfn.org/2013/10/03/defining-open-data/#:~:text=Open%20data%20is%20data%20that,%2C%20anywhere%2C%20for%20any%20purpose. Acesso em: 26 jun. 2023.

139 Sobre o assunto, ver: https://wiki.dados.gov.br/.

Dessa forma, considerando a finalidade dos tratamentos desses dados pela CNI para as relações institucionais, os seguintes dados podem ser objeto de tratamento pela CNI nessa atividade:

Exemplos de dados tratados

- Nome completo.
- Vínculo de trabalho (cargo público, filiação partidária, etc.).
- Endereço de trabalho.
- Meios de contato funcional:
  - telefone;
  - *e-mail*;
- Agenda de autoridades.
- Posicionamentos de autoridades em eventos públicos anteriores.
- Informações divulgadas por meios oficias de comunicação (Agência Senado, Notícias da Câmara e publicadas nos *sites* do Judiciário, etc.).

O tratamento desses dados é, até certo ponto, incentivado, porque é uma forma de concretização do princípio da transparência, aplicável à Administração Pública. Por essa razão, a própria LGPD reforça a possibilidade de tratamento desses dados pessoais ao prever que "o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização" (art. 7º, §3º, da LGPD).

Assim, mesmo que os dados sejam disponibilizados pelo próprio usuário, o seu tratamento deve observar os princípios da LGPD, conforme será tratado em detalhes no item 1.4.

1.2.1 BASES LEGAIS

A maioria dos tratamentos das informações para fins institucionais será enquadrada na base legal do "interesse legítimo do controlador ou terceiro interessado" e, dessa forma, passará por uma análise de proporcionalidade prévia ao tratamento. O interesse é caracterizado pela própria defesa dos interesses da indústria e, considerando os titulares envolvidos nesse tratamento, o risco envolvido é reduzido.

Para o funcionamento dessas iniciativas, a CNI também trata dados pessoais de contato e de interesse dos participantes das associações, federações e sindicatos vinculados às atividades da CNI. Em semelhança com os demais tratamentos para fins de relações governamentais, são utilizados dados públicos observados, obtidos e inferidos. Isso possibilita a construção de perfil de cadastro amplo na plataforma CRM, meio centralizado que permite o envio de informações sobre temas relevantes, convites para eventos, além de divulgação de dados sobre os próprios órgãos.

Notadamente, os princípios da LGPD e os direitos dos titulares devem ser observados. Desde os dados coletados por estarem disponíveis publicamente até os dados inferidos, não se deve aceitar o uso para fins discriminatórios, ilícitos ou abusivos, em respeito ao princípio da não discriminação. O princípio da necessidade também merece atenção para que apenas os dados essenciais às atividades exercidas sejam mantidos e atualizados.

1.2.2 ARMAZENAMENTO DE INFORMAÇÕES

Para garantir a transparência e o controle interno e externo de todas as medidas de manutenção e impulsionamento das relações governamentais, diversas informações sobre os processos atinentes às relações governamentais e de representação em outras instituições, como agências reguladoras, são registradas e armazenadas.

Como já mencionado, uma das operações de tratamentos de dados pessoais realizadas é o protocolo de registro de presença nos eventos organizados pela CNI. Assim, caso alguma autoridade participe de algum desses eventos, esse fato é registrado no cadastro da autoridade no Sistema CRM. Esse fato permite a manutenção do relacionamento com a autoridade, ajudando na definição dos temas de interesse de cada uma dessas autoridades.

Nesse mesmo sentido, na ferramenta CRM também são registradas interações entre a CNI e as autoridades. Todas as formas de relacionamento são registradas, com armazenamento de dados da autoridade diretamente e, eventualmente, dados da assessoria. Esse registro garante a memória de quem participou de cada interação e qual o conteúdo de cada um desses contatos.

É recomendável, portanto, que a ferramenta CRM seja o principal sistema utilizado para o armazenamento dos dados pessoais tratados para fins de relações governamentais. O armazenamento será mantido enquanto a autoridade ocupar cargo público ou enquanto houver justificativa legal para tanto.

Conforme recomendado anteriormente, após o fim desse período ou da atividade pública da autoridade, o gestor responsável deverá garantir a exclusão do perfil e cadastro desse titular de dados. A avaliação da necessidade de manutenção de tais perfis deve ser feita periodicamente, considerando os momentos estratégicos políticos. É recomendável que o gestor seja o único com amplo acesso a tais informações.

Dessa forma, durante todo o período de tratamento dos dados para fins de relações governamentais, as informações devem ser objeto de controle de acesso. Isso garante que o compartilhamento interno seja controlado por meio da hierarquia funcional existente dentro da CNI. Ou seja, somente funcionários com hierarquia mais alta podem autorizar o acesso dessas informações por colaboradores em posição de menor gestão.

1.2.3 PASSO A PASSO APÓS RECEBIMENTO DE DOCUMENTOS

As relações institucionais são vias de mão dupla, por isso, diversas vezes, a CNI também recebe representantes e documentos com interesses de outros agentes. Frequentemente esses documentos contam com dados pessoais de interessados, autores, autoridades, entre outros que podem se relacionar de alguma forma com a temática.

Contudo, o processo de recebimento dessas informações é descentralizado, no sentido de que qualquer representante do Sistema Indústria é capaz de receber esses dados. Por isso, deve ser adotado método de registro e descarte desses documentos para garantir que, caso existam dados pessoais, o tratamento desses seja lícito.

Passo a passo após o recebimento de documentos de relações institucionais

- Recebimento de documento por área com relacionamento com o autor.
- Verificar se no documento existem dados pessoais.
- Caso existam dados pessoais, verificar se as informações são necessárias.
- Cadastrar o documento conforme regras da área, inclusive sistema utilizado pela área/preferência pela ferramenta CRM.
  - Se os dados não forem necessários, garantir o descarte dessas informações.
- Determinar o nível de acesso a tais documentos e informações presentes.
- Enviar cópia de documento para Unidade(s) Responsável(eis) por relacionamento com Poder Executivo.
  - A unidade deverá atualizar os cadastros afetados por esse documento, em especial autoridades.
- Eliminar documento após término da finalidade e cumprimento com as obrigações legais e regulatórias pertinentes.

1.3 EXERCÍCIO DE DIREITOS EM PROCESSOS ADMINISTRATIVOS OU JUDICIAIS

Como parte do fortalecimento da relação e interesses da indústria, a CNI busca atuar estrategicamente em ações que sejam de relevância ao setor industrial. Isso se deve em especial porque a CNI é legitimada ativa para propor ações de controle concentrado perante o Supremo Tribunal Federal (STF), além de atuar em demais tribunais superiores, como o Superior Tribunal de Justiça (STJ) e Tribunal Superior do Trabalho (TST).

Os dados tratados para tal finalidade são os dados de conhecimento público porque, em regra, os atos processuais são públicos, com exceção das normas processuais que impõem, quando for o caso, sigilo e segredo judicial.

Exemplos de dados tratados[140]

- Número do processo.
- Partes.
- Terceiros interessados (*amici curiae*, litisconsortes, etc.).
- Juiz ou relator.
- Matéria dos casos (assunto).
- Fase.
- Vara/turma.
- Comarca/foro.
- Instância.
- Natureza.
- Valor da causa.
- Valor das custas processuais e honorários.
- Data de distribuição.
- Movimentações processuais.
- Escritórios responsáveis, de parceiros e da parte contrária.

Assim, são tratados dados como juiz e ou relator, justificados por meio das bases legais como o exercício regular de direitos e cumprimento de obrigações legais ou regulatórias. O armazenamento de dados também é justificado, pois necessário para a defesa em processos judiciais, a fim de ver assegurados os direitos relacionados ao contraditório e à ampla defesa.

Como produtos do acompanhamento e publicidade dos interesses da Confederação, estão a Agenda Jurídica da Indústria e o Boletim Jurídico da Indústria. O primeiro tem o objetivo de tornar pública a atuação da CNI e o posicionamento do setor acerca de importantes ações em julgamento no STF, enquanto o segundo publica trimestralmente as principais informações jurídicas da indústria.

Nesse sentido, é possível ocorrer a contratação de consultoria e demais serviços advocatícios para auxílio nas atividades concernentes ao exercício de direitos, como a realização de diligências.

No ponto, dados das empresas e prestadores de serviços contratados podem envolver nomes de pessoas físicas e jurídicas, valores financeiros da contratação e causas. Assim, também é possível o compartilhamento de dados para a execução dos serviços contratados e exercício regular de direitos quanto aos dados das partes envolvidas nos processos.

140 A listagem proposta não é taxativa, mas antes exemplificativa, que compreende tipos de dados relacionados a processos do contencioso ordinário e processos de representação de interesses.

Por isso, é recomendável a celebração de Acordos de Processamento de Dados (DPA), documentos a serem firmados, à parte ou como adendos a contratos já existentes, entre controladores e operadores. Neles, deve-se ter a delimitação do escopo e regras explícitas da atividade contratada e pode envolver questões como níveis de segurança, auditoria, e identificação de suboperadores, por exemplo.

Como essas modalidades de dados demandam o seu armazenamento por um período maior de tempo, em razão dos prazos prescricionais ou decadenciais relativos aos processos, medidas como pseudonimização ou anonimização dos dados pessoais são relevantes medidas de salvaguarda de proteção dos dados.

1.4 TRATAMENTO DE DADOS DISPONÍVEIS PUBLICAMENTE

O tratamento de dados públicos permeia tanto as atividades desempenhadas para fins de relações institucionais quanto para o exercício de direitos em processos administrativos e judiciais. Tais informações podem compreender tanto dados "ordinários" – não sensíveis – como foto, nome, perfil das redes sociais, *e-mail* profissional, cargo, etc., quando dados sensíveis, como informações sobre filiação partidária e dados sobre opinião política.

Não obstante se tratem de dados que possuem acesso livre por terceiros, o tratamento de dados "públicos" ainda gera amplo debate, sendo principalmente divididos em duas categorias: i) dados tornados manifestamente públicos pelo titular; ii) dados cujo acesso é público.

A primeira categoria de dados possui previsão específica na LGPD, que aduz que os dados não sensíveis tornados manifestamente públicos pelo titular dispensam a coleta de consentimento, devendo ser resguardados os direitos do titular (art. 7º, §4º). De acordo com o dispositivo, também devem ser respeitados os princípios da lei geral de proteção de dados, sendo necessário considerar o contexto que os dados foram disponibilizados.[141]

Ademais, quando tratados dados cujo acesso é público, nos termos do art. 7º, §3º, da LGPD, é necessário considerar os interesses públicos que nortearam a disponibilização das informações. Para garantir que o tratamento de dados dessa categoria seja realizado em cumprimento com o previsto na LGPD, defende-se que os dados de acesso público devem ser tratados com boa-fé, devendo o tratamento ser compatível com as legítimas

141 FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. **Curso de proteção de dados pessoais**: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 195.

expectativas do titular de dados, assim como a finalidade para a qual os dados foram disponibilizados.[142]

No tratamento de dados "públicos", portanto, existem duas formas de se disponibilizar as informações, quais sejam, pelo próprio usuário ou por outros motivos, como para cumprimento da Lei de Acesso à Informação, legislação eleitoral (no caso de candidatos a cargos públicos), entre outros. Independentemente da forma como o dado foi disponibilizado, fato é que um dos aspectos centrais na avaliação sobre a possibilidade de se tratar o dado depende de uma cuidadosa análise do princípio da finalidade.

Nesse sentido, vale mencionar o documento produzido pelo *Article 29 Data Protection Working Party*, "*Opinion 03/2013 on purpose limitation*,"[143] que apresenta alguns requisitos para que seja verificada a compatibilização de finalidades quando do tratamento de dados. Entre eles, o grupo destaca a necessidade de observar:

- a relação entre as finalidades para as quais os dados pessoais foram recolhidos e os objetivos do tratamento de dados realizado posteriormente;
- o contexto em que os dados pessoais foram recolhidos e o expectativa dos titulares dos dados quanto à sua utilização posterior;
- a natureza dos dados pessoais e o impacto do seu tratamento posterior aos titulares dos dados; e
- as salvaguardas adotadas pelo responsável pelo tratamento para assegurar um tratamento justo e para impedir qualquer impacto indevido sobre os titulares dos dados.

Por fim, em relação aos dados sensíveis que possuem relação com a opinião política do titular, alguns cuidados adicionais devem ser tomados. Tal fato decorre da natureza sensível desse dado e o potencial discriminatório e de restrição de direitos dos titulares que o tratamento indevido desses dados pode acarretar.

Por esse motivo, ainda que não exista uma restrição expressa da legislação em relação ao tratamento desse tipo de dado que tenha sido tornado público, fato é que a reutilização desses dados deve ter um cuidado ainda maior com o princípio da finalidade. Além disso, os princípios da adequação e finalidade[144] possuem importante papel combinados com o princípio da necessidade. Assim, a partir desses princípios, a utilização secundária de dados públicos que podem envolver informações sobre preferências políticas devem ser acompanhadas por perguntas como:

142 FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais**: Fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 195.

143 EUROPEAN COMISSION. **Article 29 Data Protection Working Party**: opinion 03/2013 on purpose limitation. 2 abr. 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 26 jun. 2023.

144 INTERNETLAB. **Proteção de dados nas eleições: democracia e privacidade.** set. 2020. p. 16. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2020/09/internetlab_protecao-de-dados-nas-eleicoes.pdf. Acesso em: 26 jun. 2023.

- As finalidades informadas ao titular são compatíveis com a operação de tratamento pretendida?
- O contexto para o qual os dados foram fornecidos inicialmente é compatível com o pretendido com a operação de tratamento?
- Existem outras formas menos invasivas de se atingir as mesmas finalidades?
- Os dados tratados são proporcionais e não excessivos?
- O titular tem a expectativa de que os dados coletados sejam utilizados para essa finalidade?
- O titular tem conhecimento de que os dados podem estar sendo tratados para esses propósitos?

Afinal, a depender das respostas apresentadas para esses questionamentos, deve-se avaliar se os dados podem ser tratados ou não. Por exemplo, um ocupante de um cargo político tem a expectativa de que seu perfil seja formado pelos representantes das empresas e que ele inclua seu partido político, bem como as propostas apresentadas em sua campanha. Contudo, mais sensível é a informação sobre a sua orientação, pois essa informação tem um potencial discriminatório elevadíssimo e pode ser considerada excessiva.

Portanto, a CNI deve ter cuidado redobrado ao formar os "perfis" das autoridades, para que não sejam tratadas informações que violem os princípios anteriormente referidos. Ademais, deve ser realizado o RIPD para assegurar que os riscos do tratamento de dados pretendido não sejam exacerbados e que salvaguardas sejam adotadas, ou mesmo que a necessidade de realização da atividade de tratamento seja reavaliada.

2 PROTOCOLO SENAI E SESI

2.1 INTRODUÇÃO

O SENAI[145] e o SESI[146] são serviços sociais autônomos, semelhantes em sua estrutura e conformação, embora tenham finalidades distintas: enquanto o primeiro[147] é serviço social de formação profissional, o segundo[148] é voltado à prestação de serviço social.

Ambos contam em sua governança com a administração superior exercida pela CNI (conforme fora atribuído por suas leis de regência) à qual são vinculados, conforme recepção advinda do art. 240 da CRFB.[149] Além disso, cada um deles é conformado por órgãos nacionais, normativos (conselhos nacionais) e administrativos (departamentos

145 Conforme o Regimento Interno do SENAI, a sua organização é disposta da seguinte maneira: "Art. 14. O SENAI, para a realização das suas finalidades, corporifica órgãos normativos e órgãos de administração, de âmbito nacional e de âmbito regional. Art. 15. São órgãos normativos: a) o Conselho Nacional, com jurisdição em todo o país; b) os conselhos regionais, com jurisdição nas bases territoriais correspondentes. Art. 16. São órgãos de administração: a) o Departamento Nacional, com jurisdição em todo o país; b) os Departamentos Regionais, com jurisdição nas bases territoriais correspondentes". SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI. **Regimento do Serviço Nacional de Aprendizagem Industrial SENAI**. 2009. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/2b/6a/2b6a9d2a-82b3-45f6-882a-631a53ee38d4/20121210151346315638i.pdf. Acesso em: 26 jun. 2023.

146 A respeito da organização do SESI e de acordo com o Regimento Interno do SESI, cita-se: "Art. 18 O Serviço Social da Indústria, para a realização das suas finalidades, corporifica órgãos normativos e órgãos de administração, de âmbito nacional e de âmbito regional. Art. 19 São órgãos normativos, de natureza colegiada: a) o Conselho Nacional, com jurisdição em todo o país; b) os Conselhos Regionais, com jurisdição nas bases territoriais correspondentes. Art. 20 São órgãos de administração, funcionando sob direção unitária: a) o Departamento Nacional, com jurisdição em todo o país; b) os Departamentos Regionais, com jurisdição nas bases territoriais correspondentes; c) as delegacias regionais, com jurisdição nas áreas que lhes competirem." SERVIÇO SOCIAL DA INDÚSTRIA - SESI. **Regulamento do Serviço Social da Indústria SESI**. 2009. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/64/94/64949dd2-4ae7-4f57-96fe-aef24c5cb2b3/sesi_regulamento_decreto_no_57375_de_2_de_dezembro_de_1965.pdf. Acesso em: 26 jun. 2023.

147 O SENAI foi criado por meio do Decreto-Lei nº 4.048/1942. BRASIL. **Decreto-lei nº 4.048, de 22 de janeiro de 1942.** Cria o Serviço Nacional de Aprendizagem dos Industriários (SENAI). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/1937-1946/del4048.htm. Acesso em: 26 jun. 2023. O seu Regimento está previsto no BRASIL. **Decreto nº 494, de 10 janeiro de 1962.** Aprova o Regimento do Serviço Nacional de Aprendizagem Industrial. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/historicos/dcm/dcm494.htm; e atualizado pelo BRASIL. **Decreto nº 6.635, de 5 de novembro de 2008**. Altera e acresce dispositivos ao Regimento do Serviço Nacional de Aprendizagem Industrial - SENAI, aprovado pelo Decreto nº 494, de 10 de janeiro de 1962. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6635.htm#art1. Acesso em: 26 jun. 2023.

148 O SESI foi criado por meio do BRASIL. **Decreto-Lei nº 9.403, de 25 de junho de 1946.** Atribui à Confederação Nacional da Indústria o encargo de criar, organizar e dirigir o Serviço Social da Indústria, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/1937-1946/Del9403.htm. Acesso em: 26 jun. 2023. O seu Regulamento está previsto no BRASIL. **Decreto nº 57.375, de 2 de dezembro de 1965**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1950-1969/d57375.htm. Acesso em: 26 jun. 2023; e atualizado pelo BRASIL. **Decreto nº 6.637, de 5 de novembro de 2008**. Altera e acresce dispositivos ao Regulamento do Serviço Social da Indústria – SESI, aprovado pelo Decreto nº 57.375, de 2 de dezembro de 1965. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6637.htm#art2. Acesso em: 26 jun. 2023.

149 Art. 240. Ficam ressalvadas do disposto no art. 195 as atuais contribuições compulsórias dos empregadores sobre a folha de salários, destinadas às entidades privadas de serviço social e de formação profissional vinculadas ao sistema sindical.

nacionais), com jurisdição em todo país; e por órgãos regionais, também normativos e administrativos, com jurisdição nas bases territoriais correspondentes.

Cabe destacar que os Departamentos Regionais possuem autonomia para administrar seus serviços, gerir seus recursos, além de determinar o regime de trabalho e relações empregatícias de seus colaboradores. Eles estão sujeitos às diretrizes e normas gerais prescritas pelos respectivos órgãos normativos nacionais (Conselhos Nacionais do SESI ou do SENAI) e à supervisão e acompanhamento exercidos pelos respectivos Departamentos Nacionais.[150]

O SENAI tem como um dos principais objetivos criar e executar programas de educação profissional, bem como cooperar no desenvolvimento de pesquisas tecnológicas para o interesse da indústria. Dessa forma, oferece "cursos de iniciação profissional, graduação e pós-graduação tecnológica para colaboradores de 28 áreas da indústria brasileira" e configura-se como o "maior complexo privado de educação profissional da América Latina."[151]

O SESI[152], por sua vez, atua no estudo, planejamento e execução de diversas medidas que possam contribuir diretamente com o bem-estar social dos trabalhadores na indústria e promoção da melhoria do padrão de vida no país.[153] Por isso, no âmbito da educação básica e continuada, busca disponibilizar cursos nas áreas de STEAM (Ciência, Tecnologia, Engenharia, Arte e Matemática) e, como medida do ramo da saúde e segurança do trabalho, desenvolve cursos, diagnósticos e consultoria às empresas industriais.[154]

Apesar de terem alguns pontos de convergência em suas atividades, as atividades desempenhadas pelo SENAI e SESI possuem distinções relevantes em relação às finalidades e à forma como dados pessoais são tratados.

Os dados utilizados pelo SESI, por exemplo, têm como finalidade o oferecimento de serviços educacionais para educação básica, além de serviços relativos à promoção da saúde, segurança, cultura e lazer do trabalhador e para formação profissional. Os dados tratados pelo SENAI, por outro lado, têm como finalidade o fornecimento de cursos para todos os níveis da educação profissional e tecnológica e o desenvolvimento de inovação

150 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. **Sistema indústria**: o motor de desenvolvimento do Brasil. Disponível em: https://www.portaldaindustria.com.br/cni/institucional/sistema-industria/#:~:text=O%20Sistema%20Ind%C3%BAstria%20promove%20e,sa%C3%BAde%20no%20ambiente%20de%20trabalho. Acesso em: 21 jun. 2023.

151 SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI. **Institucional**: educação profissional. Disponível em: https://www.portaldaindustria.com.br/senai/institucional/. Acesso em: 26 jun. 2023.

152 O SESI foi criado por meio Decreto-Lei nº 9.403/1946. BRASIL. **Decreto-Lei nº 9.403, de 25 de junho de 1946.** Atribui à Confederação Nacional da Indústria o encargo de criar, organizar e dirigir o Serviço Social da Indústria, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/1937-1946/del9403.htm. Acesso em: 26 jun. 2023.

153 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **Relato Integrado**. Brasília: SESI/DN, 2019. p. 15.

154 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **Institucional**. 2023. Disponível em: https://www.portaldaindustria.com.br/sesi/institucional/#carrossel. Acesso em: 26 jun. 2023.

voltada para a indústria, com o objetivo de capacitar sua mão de obra e aprimorar seus processos produtivos a indústria e academia.

Diante das especificidades das atividades prestadas pelo SENAI e SESI, esses três gêneros de serviços – educação, saúde e segurança do trabalhador – são considerados a seguir para recomendações de boas práticas de tratamento dos dados pessoais. Serão avaliados os tipos de dados tratados, finalidades, bases legais aplicáveis e também indicar medidas procedimentais recomendadas para minimização dos riscos envolvidos nas operações de tratamento.

2.2 TRATAMENTO DE DADOS DE ALUNOS DO ENSINO BÁSICO E MÉDIO

Entre as diversas atuações do SESI, destaca-se a oferta de educação voltada ao público infantil, fundamental e ensino médio.[155] O tratamento de dados na educação básica pode ser realizado para as mais diversas atividades cotidianas nas Instituições de Ensino, tais como realização de matrícula, controle de frequência, avaliação dos alunos, seleção de bolsistas e concessão da gratuidade regulamentar.[156]

A gratuidade regulamentar possibilita que dependentes de funcionários de empresas contribuintes do SESI possam matricular seus filhos nas unidades escolares de ensino básico de forma gratuita. Essa finalidade está prevista no Regulamento do SESI, Decreto nº 57.375/1965, e sua execução é realizada pelos Departamentos Regionais e fiscalizada pelo Departamento Nacional.

Os dados dos alunos do ensino básico e médio também são compartilhados para a concretização de obrigações perante entidades públicas e realização de estudos por órgãos de pesquisas,[157] como para a realização de censos escolares, promovidos pelo Ministério da Educação (MEC). Além disso, a cada dois anos o Departamento Nacional do SESI promove o Simulado Prova Brasil, com o intuito de acompanhar o desempenho dos alunos de Ensino

155 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **SESI Educação Infantil**. Disponível em: https://www.portaldaindustria.com.br/sesi/canais/educacao/educacao-infantil/. Acesso em: 26 jun.

156 De acordo com o art. 69 do BRASIL. **Decreto nº 57.375, de 2 de dezembro de 1965**. Que aprova o Regulamento do SESI, "O SESI vinculará no seu orçamento geral, anual e progressivamente, até o ano de 2014, o valor correspondente a um terço da receita líquida da contribuição compulsória, correspondente a vinte e sete inteiros e setenta e cinco centésimos por cento da receita bruta da contribuição compulsória, às ações mencionadas no § 2º do art. 6º, sendo que a metade deste valor, equivalente a um sexto da receita líquida da contribuição compulsória, deverá ser destinada à gratuidade". Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1950-1969/d57375.htm. Acesso em: 26 jun. 2023.

157 A respeito, confira: BACHUR, João Paulo. Proteção de dados pessoais na educação. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (Org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 478-489.

Fundamental. A iniciativa é semelhante à Prova Brasil, disponibilizada à rede pública pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) e MEC.[158]

Para a realização de matrícula e comprovação da gratuidade prevista no Decreto nº 57.375/1965, são solicitados dados pessoais e informações como:[159] i) Cópia do comprovante de residência atualizado; ii) CPF do aluno; iii) atestado de saúde para a prática de atividades físicas; iv) foto 3x4; v) tipo sanguíneo; vi) nada-consta (financeiro e biblioteca); vii) cópia do contracheque e carteira de trabalho dos pais e responsáveis; viii) formulário de gratuidade; ix) declaração de baixa renda. Ademais, além do armazenamento dessas informações, ao longo da vida escolar do(a) estudante, outros dados são coletados, tais como: i) histórico escolar; ii) dados de frequência; iii) anotações sobre o comportamento do(a) aluno(a); etc., ou seja, diversos dados de alunos e responsáveis são tratados na oferta da educação básica. Um ponto de atenção sobre esse aspecto é a grande quantidade de dados de crianças e adolescentes que são diariamente manejados para essa finalidade.

De acordo com o Estatuto da Criança e do Adolescente (ECA, Lei nº 8.069/1990), crianças e adolescentes representam um grupo vulnerável. O Código Civil, em seu art. 1.634, VII, e a própria Constituição Federal, no art. 227, também trazem importantes contornos sobre este grupo, notadamente quanto ao regime de proteção ao melhor interesse da criança e do adolescente,[160] princípio-base para a proteção de dados.

A LGPD, reconhecendo a sensibilidade desse grupo, apresenta alguns cuidados adicionais que devem ser adotados no tratamento de dados de crianças e adolescentes em seu art. 14:

i) Centralidade do melhor interesse das crianças e adolescentes no tratamento de dados.

ii) Necessidade de coleta do consentimento dos pais ou responsáveis no tratamento de dados de crianças.[161]

iii) Necessidade de disposição de informações simples, claras e acessíveis que sejam adequadas às habilidades das crianças.

iv) A minimização do fornecimento de dados de crianças e adolescentes na utilização de jogos e recursos da internet.

---

158 SERVIÇO SOCIAL DA INDÚSTRIA (SESI).**Relatório de Gestão do Departamento Nacional**. Brasília: SESI/DN, 2019. p. 73.

159 SERVIÇO SOCIAL DA INDÚSTRIA - SESI. **SESI**: educação que vai além. Disponível em: https://sesidf.org.br/?page_id=442. Acesso em: 26 jun. 2023.

160 TEIXEIRA, Ana Carolina; RETTORE, Anna Cristina de Carvalho. A autoridade parental e o tratamento de dados pessoais de crianças e adolescentes. *In*: TEPEDINO, Gustavo *et al.* (Coords.). **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019. p. 505-530.

161 Estudo preliminar da ANPD sobre as bases legais aplicáveis ao tratamento de dados de crianças e adolescentes conclui que as hipóteses previstas nos arts. 7º e 11 podem ser aplicadas ao tratamento de dados de crianças e adolescentes desde que observado o princípio do melhor interesse, conforme previsto no art. 14 da lei. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Estudo preliminar**: hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. set. 2022. p. 22. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Acesso em: 26 jun. 2023.

Em relação à utilização de outras bases legais além do consentimento, recentemente a ANPD[162] reconheceu a possibilidade de que utilizar apenas a base legal do consentimento pode apresentar uma "série de limitações jurídicas e dificuldades de aplicação prática", com riscos de se ter a coleta de um consentimento que não cumpre com o determinado pela LGPD (livre, inequívoco e específico).

Contudo, para minimizar o risco envolvido na escolha da base legal e a ausência de manifestação específica da ANPD acerca das hipóteses nas quais outras bases legais são aplicáveis, recomenda-se que a base legal do legítimo interesse seja evitada, pois ela exige o balanceamento dos interesses dos controladores e das implicações para os titulares, devendo ser avaliado se o tratamento realizado é compatível com as legítimas expectativas dos titulares e seus direitos e liberdades fundamentais.

Nesse ponto, considerando que a condição de vulnerabilidade de crianças e adolescentes exige maior atenção e proteção na coleta e tratamento de dados, o dever de cuidado dos agentes de tratamento com este grupo é ampliado consideravelmente[163] por meio do balanceamento com o princípio do melhor interesse.[164]

Tal preocupação não se estende às atividades desempenhadas no bojo da Educação de Jovens e Adultos (EJA). No entanto, os requisitos de legitimidade devem ser atendidos ao longo de todo o ciclo de vida dos dados dos estudantes.

Por fim, além do ensino básico, o SESI Educação conta diversas iniciativas como a plataforma de simulação de robôs e programação, sistema de inscrição em torneios de robótica, Portal SESI Educação, Plataforma de Aprendizagem Adaptativa repositório de boas práticas docentes da Rede SESI, que são operados por meio da execução de contrato com parceiros.

Por isso, medidas de revisão contratual como a atualização de Termos de Autorização que contenham cláusulas de privacidade e proteção de dados são importantes. Em casos de compartilhamento com empresas terceiras, recomenda-se, mais uma vez, a celebração de DPA e revisão das cláusulas contratuais, além do cuidado na seleção da empresa parceira, considerando seu histórico e reputação em relação à adoção de medidas de proteção de dados. Para tais ações, recomenda-se a consulta ao Protocolo VI, que é voltado à elaboração de acordos entre agentes de tratamento, presente na Parte II deste guia.

---

162 BRASIL. Autoridade Nacional de Proteção De Dados – ANPD. **Estudo preliminar**: hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. set. 2022. p. 13. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Acesso em: 26 jun. 2023.

163 FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais**: Fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 195. p. 250.

164 FUJIMOTO, Mônica Tiemy. Desafios do compliance de dados nas Instituições de ensino básico e superior. *In*: FRAZÃO, Ana *et al.* (Coords.). **Compliance e políticas de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2021. p. 1-173; FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais**: Fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 254.

2.3 TRATAMENTO DE DADOS PARA EDUCAÇÃO TÉCNICA E PROFISSIONAL

O SENAI atua com a formação e capacitação de profissionais nas modalidades presenciais, semipresenciais e à distância que estão à disposição do estudante e das indústrias. Os cursos são ofertados nas modalidades aperfeiçoamento/especialização profissional, graduação, iniciação profissional, micro e minicursos, pós-graduação, qualificação profissional, técnico de nível médio, além de se ter a possibilidade de oferta de cursos customizados conforme as demandas da empresa contratante.

Para oferta dessas modalidades de ensino, a entidade trata dados cadastrais dos alunos como nome, CPF, endereço, qualificação profissional, além de dados sobre desempenho acadêmico dos estudantes. Essas informações podem, inclusive, auxiliar na formação de perfis para indicação de bolsas, por exemplo.

Diante da necessidade de tratamento de uma grande quantidade de dados pessoais, deve ser realizada uma avaliação cuidadosa quanto à necessidade de coleta, compartilhamento, período de retenção e eliminação dos dados. Nesse sentido, é aconselhada uma revisão habitual sobre o fluxo dos dados e procedimentos utilizados por pelos departamentos regionais.

Ademais, a entidade compartilha dados para realização de pesquisas e avaliações regularmente desenvolvidas no âmbito do SENAI, para garantir a qualidade dos cursos fornecidos. Diante do legítimo interesse da instituição em promover melhorias de suas ações, recomenda-se especial atenção ao princípio da minimização e da necessidade para evitar a coleta de dados pessoais dos titulares que não sejam pertinentes à avaliação dos cursos. Ademais, no bojo do compartilhamento de dados para realização de pesquisas, recomendamos que a coleta de dados pessoais sensíveis seja evitada ou que eles sejam compartilhados de forma anonimizada.

O SENAI também promove pesquisas para monitorar os indicadores de desempenho dos egressos no mercado de trabalho formal e informal, além de identificar a satisfação das empresas com a instituição. Dados de 2022, por exemplo, indicaram que nove em cada dez ex-alunos da graduação tecnológica estão empregados.[165]

Assim, considerando que a finalidade do tratamento dos dados é diversa, deve ser avaliada a base legal aplicável a cada etapa do processo. A princípio, se verifica a possibilidade de utilização das bases para execução de contrato, necessária para efetuação da matrícula;

165 SERVIÇO NACIONAL DE APRENDIZAGEM – SENAI. **Nove em cada 10 ex-alunos do tecnólogo estão empregados**. set. 2022. Disponível em: https://noticias.portaldaindustria.com.br/noticias/trabalho/nove-em-cada-10-ex-alunos-do-tecnologo-estao-empregados/. Acesso em: 26 jun. 2023.

legítimo interesse para o tratamento de dados não sensíveis nas atividades quotidianas da entidade e cumprimento de obrigação regulatória ou legal pelo controlador quando existirem normas aplicáveis.

Insta ressaltar que, conforme orientando ao longo do presente guia, é importante que a LGPD seja aplicada de forma contextualizada a cada atividade analisada, isto é, que sejam consideradas além das orientações gerais as características específicas de caso a caso. Isso porque, ainda a respeito da base legal para "cumprimento de obrigação regulatória ou legal", deve-se considerar a expressão de maneira ampla, o que envolve não apenas as leis e obrigações federais, como estaduais, distrital e municipal, por exemplo.

2.4 TRATAMENTO DE DADOS DE BOLSISTAS E PESQUISADORES

O art. 53 do Regimento do SENAI[166] contém previsão específica para destinação de recursos financeiros voltados à promoção de bolsas, montagem de laboratórios de pesquisa para fins de ensino, por exemplo, ao pessoal de empresas que pagam a contribuição adicional[167] ao SENAI, conforme pelo Decreto-Lei nº 6.246/44.[168]

Entre os serviços disponibilizados pelo SENAI, podemos citar a concessão de bolsas de estudos (Instrução de Serviço 168-IS168). Para a disponibilização da bolsa são tratados dados como nome, CPF, cargo e formação acadêmica e a base legal que justifica o tratamento dos dados pessoais para concessão de bolsa podem ser o cumprimento de obrigação legal e para execução de contrato, incluindo os respectivos procedimentos preliminares.

Neste caso, são bolsas de estudos integral, de graduação ou de idiomas, por exemplo, direcionadas aos colaboradores dos Departamentos Regionais do SENAI, em especial para ex-competidores que tenham vencido torneios internacionais. Assim, a integração entre os níveis regionais e o nacional ocorre por meio do setor de Recursos Humanos do Departamento Regional no qual o colaborador faz parte, que comunica a unidade responsável. Esta emite uma carta informando sobre a premiação do colaborador que

166 SENAI. Regimento Interno: Art. 53. A contribuição adicional prevista em lei destina-se:
a) à formação, aperfeiçoamento ou especialização, inclusive por meio de bolsas de estudo, do pessoal das empresas que pagam esta contribuição;
b) ao aperfeiçoamento ou especialização de pessoal técnico, docente e administradores de ensino do SENAI, sob a forma de bolsas, de cursos e estágios;
c) à montagem de laboratórios de pesquisa para fins de ensino.

167 A contribuição adicional do SENAI recai sobre as empresas que possuem mais de 500 funcionários, as quais devem pagar uma contribuição adicional de 0,2% da folha de pagamento para o SENAI. Para mais informações, consulte: CANAL DO CONTRIBUINTE. **Tipos de contribuição**. 2023. Disponível em: https://www.portaldaindustria.com.br/cni/canais/contribuinte/sobre-a-contribuicao-compulsoria/tipos-de-contribuicao/. Acesso em: 26 jun. 2023.

168 BRASIL. **Decreto-lei nº 6.246, de 5 de fevereiro de 1944.** Modifica o sistema de cobrança da contribuição devida ao Serviço Nacional de Aprendizagem Industrial – SENAI. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/1937-1946/del6246.htm. Acesso em: 26 jun. 2023.

ganhou um curso de graduação ou de idioma, que, caso tenha interesse, deve realizar o cadastro na plataforma SENAI IS168.

Para fins de controle, o RH do Departamento Regional do bolsista (competidor) disponibiliza as informações de pedido de reembolso no sistema Abaris e o gerente executivo da Universidade Corporativa avalia o pedido. Caso aprovado, o pedido é direcionado ao setor financeiro que conduzirá os reembolsos necessários. Outro sistema também é utilizado, o *Sistame*, por meio do qual se tem o acompanhamento do desempenho do colaborador/estudante nos cursos.

O SENAI possui regras sobre a Gratuidade Regimental[169] acerca dos cursos de Formação Inicial e Continuada e os cursos Técnicos de Nível Médio, por meio das quais são estipuladas regras sobre a disponibilização dos cursos e público-alvo pretendido. Um exemplo se refere aos cursos de Aprendizagem Industrial, voltados para jovens de 14 a 24 anos, conforme disposição vigente da Consolidação das Leis do Trabalho (art. 428 da CLT).

O SESI também trata dados para concessão de bolsas e, desde 2008, incorporou em seu Regulamento uma série de dispositivos normativos para ampliação gradual da destinação de recursos à educação e à oferta de vagas gratuitas em educação básica e Continuada.[170]

Ademais, o SESI conta com uma Gerência e Educação Tecnológica que possibilita que os alunos da rede SESI, trabalhadores da indústria, profissionais da rede SESI, professores contratados ou qualquer pessoa interessada da comunidade tenham acesso à plataforma EAD (LMS). Trata-se de uma ferramenta de *webconferência*, módulo de tutoria e repositório nacional para realização de cursos e treinamentos em Educação Continuada e Educação de Jovens e Adultos.

Para cadastro, geração de certificado de conclusão de curso e divulgação dos projetos de inovação do SESI, são utilizados os seguintes dados pessoais: nome, endereço, CPF, *e-mail*, RG, telefone, profissão, data de nascimento, gênero, nacionalidade e empresa contratante.

Ademais, são realizadas operações que envolvem dados pessoais sensíveis, relativos à saúde dos candidatos (física, auditiva, fala, visual e cognitiva) e dados de adolescentes acima de 15 anos, sob a supervisão do responsável do menor.

169 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **Gratuidade regulamentar – SESI**. [2018]. Disponível em: https://www.rn.sesi.org.br/wp-content/uploads/2018/07/Metodologia-de-Apuracao-da-Gratuidade-Regimental-sesi.pdf. Acesso em: 26 jun. 2023.

170 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **Gratuidade regulamentar – SESI**. [2018]. p. 75. Disponível em: https://www.rn.sesi.org.br/wp-content/uploads/2018/07/Metodologia-de-Apuracao-da-Gratuidade-Regimental-sesi.pdf. Acesso em: 26 jun. 2023.

Nesse contexto, o tratamento de dados sensíveis pode ser realizado sob as bases legais do cumprimento de obrigação legal ou regulatória, consentimento e exercício regular dos direitos. Ainda assim, por existir um risco elevado nessas operações de tratamento, recomenda-se a elaboração do RIPD, nos termos do Protocolo III, para Avaliação de Risco, da Parte II supra, além da anonimização ou pseudonimização sempre que possível.

Ademais, o art. 33 do Regulamento do SESI pode ser indicado como norma que justifica a utilização da base legal "cumprimento e obrigação legal ou regulatória". Por meio das alíneas *a*, *d*, *p*; é possível sustentar a existência de previsão legal para a fiscalização direta ou indireta, da execução pelas administrações regionais dos dispositivos legais, regulamentares, estatutários e regimentais atinentes ao SESI e do acompanhamento e avaliação do cumprimento "pelos órgãos regionais das regras de desempenho e das metas físicas e financeiras relativas às alocações de recursos na educação e às ações de gratuidade".

Por fim, ressalta-se que o tratamento de dados sempre deve ocorrer sob observância dos princípios previstos na LGPD como a adequação, necessidade, finalidade e transparência, em consideração aos objetivos de estudo e pesquisa.[171] Assim, independentemente da finalidade almejada com o tratamento dos dados pessoais e a base legal aplicável, deve ser realizada a avaliação subjetiva da entidade a respeito do atendimento aos princípios previstos na legislação.

2.5 TRATAMENTO DE DADOS SOBRE SAÚDE E SEGURANÇA DO TRABALHADOR

O tratamento de dados sobre saúde e segurança do trabalhador é essencial para o cumprimento dos propósitos do SESI e tem como importante característica o fluxo de dados entre os Departamentos Regionais e o Departamento Nacional, conforme destacado no Protocolo Geral III.3.

171 ANPD. Guia Orientativo **Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 28 jun. 2023.

Entre os dados tratados pelo SESI, destacamos os seguintes:

- Nome de registro e nome social.
- Cargo.
- Matrícula.
- Nome Funcionário.
- Data de Nascimento.
- Sexo.
- Cor/raça.
- Contratação: data de Admissão e data de Demissão, turno.
- Estado Civil.
- Pis/Pasep.
- RG.
- CPF.
- CTPS.
- Endereço (Bairro, Cidade, UF, CEP).
- Nome da mãe e do pai do Funcionário.
- Carteira Profissional: Série, CTPS.
- Descrição Detalhada do Cargo, número, endereço Unidade, Complemento endereço, Unidade Regime de Revezamento.
- Remuneração Mensal (R$).
- Telefone Comercial e Telefone Celular.
- Escolaridade.
- Código Categoria (eSocial).
- Matrícula RH.
- Gênero Tipo de Admissão, Grau de Instrução.
- Código Atividades Perigosas (Tabela 28 – eSocial).
- Tipo Sanguíneo.
- Registro de dependentes: nome, CPF e tipo de dependente.
- Ficha clínica ocupacional.
- Anamnese.
- Resultado de exames, etc.

O Info SESI Viva+ é um sistema que faz uso dos dados do Sistema S+, Telemedicina e SESI Facilita (nome, CPF, *e-mail* e dados de saúde do público-alvo dos Sistemas de Negócio da Unidade de Saúde da Indústria do SESI/DN) para gerar indicadores, de acordo com a hierarquia e o perfil de acesso de cada usuário. A plataforma permite o acesso aos dados conforme cada fluxo específico, e pode fornecer às empresas informações como:[172]

- Indicadores de saúde e segurança do trabalho (SST).
- Alertas sobre processos e conformidades com os programas sociais.
- Indicadores de Afastamento, exames, acidentes na visão SESI, Cliente e profissionais de Saúde.

172 SERVIÇO SOCIAL DA INDÚSTRIA – SESI. **SESI para você**. 2023. Disponível em: https://sesigoias.com.br/sesi/site/Institucional.do?vo.codigo=380&v=. Acesso em: 26 jun. 2023.

- Indicadores de EPI na visão SESI e Cliente.
- Indicadores da Telemedicina na visão SESI, Cliente e profissionais de Saúde.
- Indicadores de gestão do negócio para os Departamentos Regionais – Contratos.

Logo, o Info SESI Viva+ destina-se a oferecer indicadores nacionais, regionais, de unidades operacionais e de empresas clientes, com predominância do Departamento Regional da Bahia, fornecedor e desenvolvedor da ferramenta e quem armazena os dados atualmente. Nota-se, desta forma, outro produto que demonstra o necessário compartilhamento de dados, visto que ele pertence ao Departamento Nacional.

Da mesma forma, no tratamento de dados sensíveis – como os de saúde, cor/raça – o potencial discriminatório e restritivo de direitos deve ser observado, não sendo possível aplicar bases legais mais amplas como o legítimo interesse e execução contratual, uma vez que o próprio dispositivo legal não prevê tais bases legais.

Destaca-se aspecto central quanto à limitação da base legal de tutela de saúde, porque restrita às atividades fim dos colaboradores e aos profissionais de saúde sujeitos à obrigação de sigilo. Como exemplos de atividades fim, indica-se, por exemplo, a avaliação da capacidade de trabalho do empregado, o diagnóstico médico e a medicina preventiva ou do trabalho.[173]

Logo, ainda que os dados de saúde sejam utilizados para fins de admissão de funcionários ou políticas afirmativas para pessoas com deficiência(s) (PcDs), não se pode utilizar a base legal da tutela da saúde caso esse dado não seja tratado "por profissionais de saúde, serviços de saúde ou autoridade sanitária" (art. 7°, VII, e art. 11 da LGPD).

Nesse sentido, vale considerar que tais dados sensíveis podem ser tratados por médicos no âmbito dos serviços da Segurança e Saúde no Trabalho (SST), para que sejam ofertados os serviços prestados pelos Departamentos Regionais do SESIS às empresas clientes do SESI+. Assim, nessa hipótese, a base legal da tutela da saúde seria aplicável.

Ademais, os dados de saúde também podem ser tratados de acordo com outras bases, como a do exercício regular de direitos em contrato (art. 11, II, d, da LGPD) ou prevenção de fraudes e garantia da segurança do titular (art. 11, II, d, da LGPD), desde que analisados o contexto, finalidade do tratamento e os demais requisitos legais previstos na LGPD.

173 A respeito, consultar o Código CNSaúde, em que são discutidas as bases legais aplicáveis sobre dados que envolvem a saúde dos indivíduos. CNSAÚDE. **Código de boas práticas**: proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 26 jun. 2023.

3 PROTOCOLO IEL

3.1 INTRODUÇÃO

O Núcleo Central do IEL tem como objetivo promover centros de conhecimento que permitam o desenvolvimento de carreiras, oferecendo soluções customizadas. No âmbito nacional, esse ente foi criado e atualmente é mantido pela CNI, SENAI/DN e SESI/DN,[174] e está diretamente ligado à Diretoria de Educação e Tecnologia (Diret) da CNI e estrutura suas atividades em três eixos: Tecnologia e Inovação, Educação e Qualidade de Vida.[175] No Distrito Federal e Estados, conta com Núcleos Regionais, pessoas jurídicas diferentes do Núcleo Central e que apresentam Núcleos Regionais com estatutos em conformidade ao do Núcleo Central,[176] os quais são compostos pelas Federações filiadas à CNI e demais departamentos regionais do SENAI e do SESI.

A entidade atua como agente de integração na promoção do estágio (Programa IEL de Estágio), educação executiva e gestão empresarial (Educação Executiva IEL) e incentivo a pesquisa (Inova Talentos e Inova Tec). Assim, são tratados dados de diversos perfis de titulares, envolvendo dados de colaboradores, alunos, candidatos a vagas de estágio, estudantes, profissionais e potenciais bolsistas.

A execução das atividades do IEL requer o compartilhamento de dados entre os núcleos regionais e o nacional para confecção de relatórios, como é o caso dos cursos pagos pelas instituições que envolvem a confecção de boletos e notas fiscais pelos setores financeiros. Ademais, cada uma das frentes de atuação do IEL requer o tratamento de dados para diferentes finalidades.

174 INSTITUTO EUVALDO LODI – IEL. **Estatuto Instituto Euvaldo Lodi Núcleo Central**. Brasília, 2009. Art. 1º. Disponível em: http://arquivos.portaldaindustria.com.br/app/conteudo_24/2012/07/06/133/20121101200659157217a.pdf. Acesso em: 26 jun. 2023.

175 INSTITUTO EUVALDO LODI – IEL. **Institucional**: estrutura. Disponível em: https://www.portaldaindustria.com.br/iel/institucional/estrutura/. Acesso em: 26 jun. 2023.

176 INSTITUTO EUVALDO LODI – IEL. **Estatuto Instituto Euvaldo Lodi Núcleo Central**. Brasília, 2009. Art. 25, §1º e §3º. Disponível em: http://arquivos.portaldaindustria.com.br/app/conteudo_24/2012/07/06/133/20121101200659157217a.pdf. Acesso em: 26 jun. 2023.

Assim, a seguir, avaliaremos as especificidades das principais operações de tratamento de dados realizadas pelo IEL.

3.2 TRATAMENTO DE DADOS PESSOAIS PARA FINS DE CONTRATOS DE ESTÁGIO COMO AGENTE INTEGRADOR

3.2.1 SOLUÇÕES DE ESTÁGIO PARA EMPRESAS

A oferta de soluções de estágio para as empresas tem como finalidade conectar estudantes que buscam conhecer os aspectos práticos do mercado e as empresas que buscam descobrir novos talentos e forma capital humano em conjunto com as universidades.

O sistema de estágio conta com quatro figuras centrais, que tem como objetivo principal possibilitar o desenvolvimento dos estudantes e o estreitamento da relação entre o mercado de trabalho e as universidades:[177]

Instituição de Ensino Superior (IES) Entidade dedicada à educação, regularmente constituída e autorizada ou reconhecida pelos órgãos oficiais de educação, em que o estagiário está matriculado.	*Agentes de Integração* São entidades, públicas ou privadas, contratadas pelas instituições de ensino e/ou pelas partes concedentes de estágio, mediante condições acordadas em instrumento jurídico apropriado que visam, principalmente, a auxiliar no processo de aperfeiçoamento do estágio e realizar o acompanhamento administrativo, por exemplo, além de contribuir na busca de espaço no mercado de trabalho, aproximando, instituições de ensino, partes concedentes e estudantes.
Parte Concedente Quem oferece o estágio, ou seja, as pessoas jurídicas de direito privado e os órgãos da Administração Pública direta e indireta, autárquica e fundacional da União, dos estados, do DF e dos municípios, bem como profissionais liberais de nível superior, devidamente registrados em seus respectivos conselhos.	***Estagiário*** Estudante regularmente matriculado e com frequência nos cursos de educação superior, profissional, de ensino médio, da educação especial, nos anos finais do ensino fundamental, na modalidade profissional da EJA.

177 INSTITUTO EUVALDO LODI – IEL. **Lei de Estágio**: tudo o que você precisa saber. Brasília: IEL/NC, 2010.

Para possibilitar o desenvolvimento da atividade de estágio, é necessário o compartilhamento de informações que incluem dados pessoais entre esses quatro atores, como por exemplo:

Dados compartilhados para fins de Estágio

- **Estagiário**:
  - Nome.
  - *E-mail*.
  - RG.
  - CPF.
  - Endereço (CEP).
  - Telefone.
  - Data de nascimento.
  - Cargo e horário de prestação das atividades.
  - Foto (avatar).
  - Raça.
  - IEs ao qual é vinculado.
  - Curso (com data de início e previsão de fim do curso; ano/semestre atual do curso; número de matrícula; identificação se é bolsista ou não; período de estudo).
  - Cursos extracurriculares: idiomas, tecnologias, ferramentas (tipo de conhecimento, nome da formação, IEs, ano de início, ano de término).
  - Remuneração da bolsa estágio.
  - Arquivos anexados (portfólio, currículos, que podem conter experiência de trabalhos anteriores, como o nome da empresa, data de início e término, função, atividades desempenhadas, etc.).
- **Responsáveis Empresa e processo seletivo:**
  - Nome.
  - CPF.
  - Cargo.
  - *E-mail*.
- **IEs:**
  - Dados de identificação institucionais: como nome, CNPJ; endereço (CEP). telefone e *e-mail*.
  - Coordenador do curso ou outro responsável legal: nome, CPF, cargo, *e-mail*, formação e número de classe.

Em relação aos dados pessoais não sensíveis, as bases legais comumente utilizadas envolvem a execução de contratos, bem como o cumprimento de obrigações legais que exigem a coleta de dados, como no caso de adolescentes, os quais serão trabalhados em item posterior.

É crucial ressaltar que, quando as informações sensíveis estiverem envolvidas, deve-se manter um registro cuidadoso das hipóteses que justificam o tratamento, sendo necessária detalhada avaliação acerca da necessidade e possibilidade de coleta e tratamento desse tipo de dado. Também recomendamos que seja elaborado o RIPD, especialmente se for tratado um grande volume de dados sensíveis.

Tendo em vista a existência de processos de adequação à LGPD em curso nas entidades e órgãos do Sistema Indústria, a revisão contratual e termos aditivos que prevejam de forma bem definida o escopo das finalidades, dos tipos de dados tratados e possíveis compartilhamentos são medidas importantes a serem implementadas. Entre os contratos que podem ser revisados, é possível mencionar os convênios envolvendo o IEL como agente de integração e outros contratos com parceiros que são realizados no bojo da entidade, envolvendo dados pessoais.

Recomenda-se a edição de contratos ou DPAs que vinculem os parceiros a deveres de proteção, confidencialidade e sigilo de base de dados e demais informações a que tenham acesso, além de solicitar que sejam adotadas medidas técnicas e administrativas capazes de garantir a segurança das informações contra possíveis incidentes de segurança também devem ser consideradas. Entre os tópicos a serem observados na elaboração de cláusulas contratuais, sugerimos que os pontos apresentados no Protocolo VI sejam considerados:

- Glossário com terminologia da LGPD.
- Duração das atividades de tratamento.
- Indicação de agentes de tratamento.
- Finalidades específicas do tratamento de dados.
- Vedação à utilização de dados pessoais sem ciência ou autorização da controladora.
- Exigência de adequação das partes do contrato à LGPD.
- Vedação ao compartilhamento de dados pessoais e obrigatoriedade de notificação à parte caso o compartilhamento seja necessário.
- Obrigação de registro de informações.
- Obrigação de implementação de medidas técnicas e administrativas que garantam a segurança dos dados tratados.
- Possibilidade de realização de auditorias para demonstração de cumprimento da legislação.
- Deveres de confidencialidade.
- Periodicidade de atualização de informações do contrato.
- Hipóteses de transferência de dados.
- Obrigatoriedade de elaboração de plano de incidentes envolvendo dados pessoais.
- Procedimentos de destruição e devolução de dados pessoais;
- Obrigatoriedade de notificação em caso de determinações oficiais que obriguem o fornecimento de dados pessoais.
- Obrigatoriedade de contratação de DPO por operador.

Ademais, deve-se avaliar a possibilidade de, na medida do possível, os parceiros se comprometerem a não armazenarem cópias ou *backups* das informações compartilhadas e devolverem ao IEL documentos que contenham os dados pessoais, como etapa do encerramento do tratamento dos dados e sua consequente eliminação.

3.2.2 SISTEMA NACIONAL DE ESTÁGIO

Também como parte das iniciativas do IEL para garantir a integração entre indústria, universidade e novos talentos, o Sistema Nacional de Estágio é uma plataforma desenvolvida pelo IEL para gestão de estágios, garantindo a divulgação de vagas e centralizando o cadastro para processos seletivos de estágio.

Por meio do sistema, as empresas podem dispor de alguns serviços como a Emissão de Documentos (Declaração de Conclusão de Estágio e Declaração de Horas; Termo de Realização de Estágio (atividades e avaliação); Avaliação de Estágio), e contar com modelos de recibos de pagamento de bolsa e auxílio transporte, por exemplo.[178]

As funcionalidades do Sistema estão todas de acordo com a Lei do Estágio (Lei nº 11.788/08), de tal forma que o IEL pode atuar como:[179]

a) Agente de integração, quando contratado por instituição de ensino e/ou pelas partes concedentes de estágio, mediante condições acordadas em instrumento jurídico apropriado, aproximando instituições de ensino, partes concedentes e estudantes.
b) Parte concedente, quando oferece vaga de estágio.

Ainda que atue também como parte concedente, o IEL estará sempre atuando como agente de integração por meio do sistema nacional de estágio. Entre as obrigações do agente de integração, cabe a esse ator cadastrar os estudantes. Nesse momento, é necessária a coleta de vários dados pessoais, entre eles:

- Dados de identificação (data de nascimento, CPF, nome completo, nome da mãe, *e-mail*, número de celular, nacionalidade, sexo, informações sobre deficiência, estado civil, RG).
- Endereço.
- Dados escolares (universidade/escola, curso, perspectiva de formação).

Essas informações são necessárias para a elaboração do Termo de Compromisso de Estágio, além de identificação de vagas compatíveis com o cadastrado. Assim, o tratamento dos dados pessoais terá base, majoritariamente, no cumprimento de obrigações legais e regulatórias e na execução de contrato ou procedimentos preliminares, sendo o titular parte da relação contratual.

178 INSTITUTO EUVALDO LODI – IEL. **Manual do SNE**. Disponível em: https://ielal.com.br/public/documentos/manual-sne-empresas-novo.pdf. Acesso em: 26 jun. 2023.

179 INSTITUTO EUVALDO LODI – IEL. **Cartilha sobre a Lei de Estágio**: tudo o que você precisa saber. 2010. Disponível em: https://sne.iel.org.br/sne/down/cartilha_estagio_IEL.pdf. Acesso em: 26 jun. 2023.

Entre os dados coletados, estão os dados sensíveis sobre candidatos identificados como PcDs. Essa informação é necessária para o cumprimento de obrigação legal, tendo em vista que a Lei do Estágio assegura o percentual de 10% (dez por cento) das vagas de estágio oferecidas pela parte concedente para pessoas com deficiência (art. 17, §5º, da Lei nº 11.788/2008).

Nesse caso, por se tratar de dados sensíveis, independentemente da base legal utilizada, recomenda-se a elaboração de um Relatório de Impacto, nos termos do Protocolo Geral III supra, assim como cuidadosa avaliação sobre os princípios da necessidade, finalidade e possibilidade de pseudonimização desses dados.

3.2.3 TRATAMENTO DE DADOS DE ADOLESCENTE

Como considerado anteriormente, alguns programas de estágio podem envolver menores de idade. A respeito do tema, a ANPD, publicou o seguinte enunciado, em 24 de maio de 2023, a respeito do tratamento de dados pessoais desse público:[180]

> O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da Lei Geral de Proteção de Dados (LGPD), desde que observado o seu melhor interesse, a ser avaliado no caso concreto, nos termos do caput do art. 14 da Lei.

Por isso, é recomendável que os processos que envolvam dados de adolescentes sejam objeto de cuidado adicional para garantir a efetiva necessidade de utilizar as informações até então requisitadas, evitando-se o acúmulo de dados desnecessários aos fins pretendidos, sempre considerando o melhor interesse dos adolescentes, nos termos do caput do art. 14 da LGPD. Ademais, por hipótese, caso sejam tratados dados de crianças, deve ser coletado o consentimento dos pais ou responsável legal, nos termos do art., 14, § 1º, da LGPD.

Técnicas de anonimização ou pseudonimização são recomendáveis para um controle mais seguro sobre o acesso e identificação dos menores.

3.2.4 DESAFIO 4.I

O Desafio 4.i é desenvolvido para que as empresas, estudantes e instituições de ensino sejam aproximadas por meio do alinhamento da teoria e prática: são propostos desafios das empresas a serem solucionados por estudantes acompanhados de mentores das

180 BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. **Estudo preliminar**: hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. set. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Acesso em: 26 jun. 2023.

universidades.[181] A premiação é uma oportunidade para que jovens profissionais apresentem seus projetos para empresas, possibilitando a sua entrada no mercado de trabalho.[182]

Assim, configura-se como uma iniciativa importante que busca reconhecer e incentivar o desenvolvimento de projetos inovadores na jornada acadêmica e profissional de jovens.

As empresas participantes selecionam os cursos de ensino técnico ou superior que poderão participar do desafio. Essa seleção é essencial, uma vez que somente estudantes regularmente matriculados e frequentando as aulas de tais instituições poderão se inscrever para o desafio.

As empresas também indicam quem são os tutores técnicos escolhidos por elas para o auxílio aos estudantes. Esse processo conta com o envio das seguintes informações dos tutores para o Núcleo do IEL responsável pelo desafio:

1. CNPJ.
2. Razão social.
3. Nome do responsável
4. Cargo do responsável.
5. Contato do Responsável.
6. Tema do desafio.
7. Descrição do desafio.

Além disso, é assinado um termo de Adesão ao Desafio Estágio 4.i. e, em seguida, é elaborado e publicado regulamento com regras de participação, onde são disponibilizados os *links* para inscrição. O processo de inscrição de estudantes é feito por formulário *on-line*, momento em que são coletadas as seguintes informações:

1. Informações básicas de identificação (nome completo, CPF, data de nascimento, gênero, estado civil).
2. Informações para contato (telefones para contato e *e-mail*).
3. Formação acadêmica (instituição de ensino, curso matriculado).

Como se pode observar, o processamento desses dados é essencial para verificar a identidade de todos os inscritos, além de garantir o cumprimento dos requisitos de participação. As informações também são imprescindíveis para avaliação do desafio, inclusive sobre as formas de contato com mentores técnicos das instituições parceiras.

181 INSTITUTO EUVALDO LODI – IEL. **Regulamento**: desafio 4.i. Disponível em: https://ielsc.org.br/pt-br/file/21329/download?token=SM01ON75. Acesso em: 26 jun. 2023.

182 INSTITUTO EUVALDO LODI – IEL. **Desafio 4.i premia estudantes que solucionaram demandas das indústrias**. 25 nov. 2023. Disponível em: https://noticias.portaldaindustria.com.br/noticias/educacao/desafio-4i-premia-estudantes-que-solucionaram-demandas-das-industrias/. Acesso em: 26 jun. 2023.

Paralelamente, também é desenvolvido o processo seletivo de mentores, cuja seleção é de responsabilidade do IEL. As vagas são divulgadas em alguma das plataformas parceiras do IEL (PandaPé ou vagas.com), em que o processo seletivo é desenvolvido. Para essa finalidade, são tratadas as seguintes informações:

1. Informações de identificação (nome completo, CPF, data de nascimento, estado civil, gênero).
2. Informações para contato (números de telefone, *e-mail*).
3. Endereço completo.
4. Currículo com formação acadêmica e experiência profissional.
5. Outras competências relevantes.

Dessa forma, pode-se aplicar a base legal da execução do contrato – incluindo os procedimentos preliminares, bem como o legítimo interesse por parte do IEL. Conforme exposto no Protocolo III, item III.4. Avaliação do legítimo interesse, sendo necessária avaliação da necessidade e proporcionalidade do tratamento realizado.

A base legal do legítimo interesse pode ser utilizada especialmente para a posterior distribuição de conteúdos informativos para participantes. Contudo, é necessário fornecer a possibilidade de os titulares pedirem para que o tratamento seja interrompido, *opt-out*, e as comunicações devem ser relacionadas ao propósito do desafio.

Ademais, cumpre ressaltar que os termos de uso das plataformas parceiras do IEL devem deixar claras as finalidades do tratamento de dados realizado, conforme será abordado em detalhes no tópico III.4. infra., sendo responsabilidade do IEL deixar claro para os participantes quais plataformas são utilizadas, os dados tratados e a finalidade.

Os regulamentos e termos a serem firmados também devem prever as condições pelas quais os dados produzidos em relatórios técnicos, produtos e tecnologias, por exemplo, serão tratados, sendo razoável que o IEL possa usá-los para divulgação ou reprodução para "fins de multiplicação do conhecimento no âmbito de suas finalidades institucionais, desde que não se trate de informações sigilosas ou confidenciais".[183]

3.2.5 PRÊMIO IEL DE ESTÁGIO

O Prêmio IEL de Estágio reconhece ideias de estagiários e jovens talentos que implementam projetos inovadores na jornada acadêmica e profissional. A premiação é realizada em três categorias: projetos inovadores, empresa inovadora e educação inovadora.[184]

183 INSTITUTO EUVALDO LODI – IEL. **Regulamento**: desafio 4.i. (cláusula 10, item c). Disponível em: https://ielsc.org.br/pt-br/file/21329/download?token=SM01ON75. Acesso em: 26 jun. 2023.

184 INSTITUTO EUVALDO LODI –IEL. **Prêmio IEL de Estágio 2022**. 2023. Disponível em: https://www.portaldaindustria.com.br/iel/canais/iel-estagio/premio-de-estagio/. Acesso em: 26 jun. 2023.

Todas as inscrições são feitas por meio de modelos de formulários disponíveis *on-line* e com envio para *e-mail* disponibilizado no *site* respectivo. Para todas as categorias, é requisitado um termo de autorização de uso de imagem sem ônus para as entidades do Sistema Indústria, em especial, o próprio IEL, para atualização do Banco de Imagens e para veiculação em materiais de divulgação utilizados pelo Sistema.

Para a inscrição nas categorias projeto inovador e empresa inovadora, é necessária a coleta de dados pessoais dos participantes da equipe. Os dados coletados são: **nome, *e-mail*, telefone e função dentro da empresa.** Para essas categorias, ainda é necessário o preenchimento de termo de adesão que requer a coleta do **nome, cargo, telefone e *e-mail* do responsável pela participação, assim como o nome do responsável legal da empresa.**

Já para a categoria de educação inovadora, o formulário de submissão requer os dados do responsável pelo processo, que incluem: **nome completo, cargo, telefone para contato e *e-mail*. Esses dados também devem ser fornecidos no termo de adesão**.

A respeito da base legal, verifica-se que os tratamentos dos dados do desafio se enquadram na base legal da execução contratual, mas o legítimo interesse pode ser utilizado para outras operações de tratamento de dados operacionais e para o envio de informações promocionais. Novamente, recomendamos que seja utilizado o mecanismo "*opt-out*" caso sejam enviadas mensagens promocionais e que o teor do conteúdo seja vinculado ao objetivo da premiação.

Para a divulgação do resultado, sugere-se que apenas o nome seja divulgado, evitando-se outras informações excessivas como o CPF. Caso seja divulgada uma lista com diversos candidatos, ela também pode ser elaborada por meio da pseudonimização dos participantes. Por exemplo, pode-se criar um número de inscrição para dificultar a identificação dos participantes e apenas o ganhador ter seu nome divulgado.

Ademais, a autorização de uso de imagem deve deixar claro quando e quais imagens serão utilizadas. Não se recomenda a utilização de fotos das redes sociais dos premiados sem a sua autorização.

Os dados do titular também podem ser utilizados para a divulgação do resultado do concurso, estando essa operação amparada pela base legal da execução do contrato. Deve-se evitar, contudo, que o envio de informações sobre o concurso possibilite a identificação de outros candidatos ou candidatas, sendo recomendável a utilização da ferramenta "cópia oculta" caso seja necessário o envio de *e-mails* para um grupo de pessoas.

Além do mais, o titular deve ser amplamente informado sobre os tratamentos de dados e as finalidades deles por meio do regulamento dos prêmios disponibilizado anualmente.

3.3 TRATAMENTO DE DADOS PARA CONCESSÃO DE BOLSA DE ESTUDANTES E EGRESSOS DA ACADEMIA

3.3.1 INOVA TALENTOS

O Inova Talentos objetiva fomentar projetos de inovação em empresas as quais devem inscrever seus projetos e, caso aprovados, são ofertadas bolsas de fomento tecnológico e extensão inovadora aos jovens talentos.

Aqui há atuação central do IEL/NC-SP (atualmente, o único exemplo de filial ao Núcleo Central, sendo este localizado em Brasília-DF, visto que os demais estados brasileiros contam com Núcleos Regionais) que, em apoio aos demais núcleos regionais, atuam no processo de divulgação, recrutamento e seleção.

Os dados envolvidos referem-se inicialmente ao cadastro dos participantes, entre os quais:

Bolsista

- Nome.
- RG.
- CPF.
- Data de nascimento.
- Local de nascimento.
- Nome do pai e da mãe.
- PIS/Pasep.
- NIT.
- Cor/raça.
- *E-mail.*
- Telefone.
- Endereço.
- Título de eleitor e comprovante da última votação.
- Certificado de alistamento militar, quando for o caso.
- Registro Nacional de Estrangeiro (RNE), quando for o caso.
- Cópia autenticada do passaporte, no caso de bolsista estrangeiro.
- Documentos acadêmicos como: atestado de matrícula vigente para estudantes e cópia do diploma da formação mais recente e dados bancários completos, cuja titularidade seja do bolsista.

Empresa (Coordenador e executor do projeto):

- Nome.
- CPF.
- Cargo.
- *Link* de acesso ao currículo *Lattes.*
- *E-mail.*
- Formação.
- Titulação do executor.

Neste programa, o compartilhamento dos dados dos alunos ocorre com outras instituições que tenham celebrado o Acordo de Cooperação com o IEL e/ou empresas que tenham celebrado Acordos de Parceria. Isso ocorre para que o IEL/NC-SP (filial do Núcleo Central do IEL no estado de São Paulo) realize o cadastro dos profissionais nas plataformas das Entidades parceiras, como o CNPq, IPT, FIPT e de outras Entidades parceiras. Sendo assim, a base legal aplicável em geral é o legítimo interesse, execução de contrato, além de eventual cumprimento de obrigação legal e regulatória.

Em relação ao tratamento de dados sensíveis, quando não se tratar de obrigação legal ou regulatória, recomenda-se solicitar o consentimento para que esses dados sejam tratados, sendo necessária a realização de um RIPD. Conforme já exposto no item VII.4, do Protocolo Tratamento de Dados para Realização de Eventos, a utilização do consentimento deve ser realizada com alguns cuidados, em especial, deve ser garantido que os direitos do titular relativos ao consentimento sejam atendidos.

Ao longo da seleção, o IEL conta com um banco de informações que possibilita a identificação e coleta dos dados da empresa e dos alunos. Entre os parceiros da iniciativa, estão o CNPq, IPT e as empresas seguradoras, com as quais os dados cadastrais dos bolsistas podem ser compartilhados.

Observa-se que os dados do tutor e dos gestores da área são tratados para permitir a execução contratual; e os dos bolsistas também são tratados a partir da manifestação de interesse na bolsa. Os dados dos representantes legais das empresas são requisitados para comprovação da cadeia de poderes de representação.

Ademais, recomenda-se que os contratos e termos aditivos prevejam expressamente o escopo do compartilhamento de dados, com a descrição de todas as etapas dos serviços que os requisitam e com quem serão compartilhados, por exemplo. Nos convênios firmados, recomendamos a inclusão de cláusulas contratuais que vinculam as partes a obrigações relacionadas à proteção de dados, nos mesmos termos recomendados no item “2.2.a.” supra.

3.4 EDUCAÇÃO EXECUTIVA E GESTÃO EMPRESARIAL

Este serviço busca aprimorar a capacitação técnica de funcionários de empresas, com o oferecimento de cursos *on-line* gratuitos ou pagos a serem ofertados para toda a comunidade.

A sua operacionalização se dá inicialmente com a divulgação de um *link* em que são apresentados os cursos ofertados, pelo qual os usuários precisam realizar um cadastro na plataforma *Konviva* e, então, selecionar os cursos desejados.

Os dados cadastrais envolvem: **nome, *e-mail*, RG, CPF, endereço, telefone, data de nascimento**.

Com tais informações, os serviços são disponibilizados e é possível providenciar a respectiva gestão até a conclusão do curso, com consequente emissão de certificado, caso atendidos os requisitos próprios de cada. Ademais, se os cursos forem pagos há o compartilhamento das informações com a área para que seja providenciada a emissão de boletos e notas fiscais, sendo aplicável a base legal do cumprimento de obrigação legal ou regulatória.

Além disso, o Treinamento *in Company* permite a prestação de serviços pelos núcleos regionais do IEL na localidade das empresas, de forma que os dados de identificação dos alunos apenas são necessários para acesso à plataforma e geração de certificados. Também é possível o compartilhamento de dados com a empresa contratante, caso se tenha requisição.

Outros serviços ofertados dizem respeito à promoção de Eventos *On-line*, com diversos webinários voltados a promover novas iniciativas e expandir a rede de contatos do IEL, e a prestação de consultoria em gestão do IEL, destinado à oferta de um atendimento especializado que traz soluções para alavancar resultados e fornece oportunidades de melhorias para uma organização.[185]

Portanto, considerando que as empresas buscam o IEL para que seus serviços sejam ofertados, a base legal que permite o tratamento de dados pessoais primordialmente é a execução de contratos (quando o titular for parte) e o legítimo interesse, sendo recomendável a celebração de DPA com as empresas nas quais ocorre o compartilhamento dos dados. Além disso, uma vez que o IEL também acaba possuindo relação com o titular, intermediada pela empresa contratante da plataforma, também existe um contrato entre a IEL e o estudante.

Conforme mencionado nos tópicos supra, caso se pretenda enviar informativos sobre outras iniciativas do IEL, a base legal do legítimo interesse pode ser utilizada, devendo ser facultado ao usuário o *opt-out*.

185 INSTITUTO EUVALDO LODI – IEL. **Educação executiva**. 2023. Disponível em: https://loja.edu-executiva.iel.org.br/. Acesso em: 26 jun. 2023.

CNI
Robson Braga de Andrade
Presidente

DIRETORIA JURÍDICA – DJ
Cassio Augusto Muniz Borges
Diretor Jurídico

Gerência Executiva de Estratégia Jurídica
Alexandre Vitorino Silva
Gerente Executivo de Estratégia Jurídica

Gerência de Consultoria
Fabiola Pasini Ribeiro de Oliveira
Gerente de Consultoria

Cassio Augusto Muniz Borges
Fabiola Pasini Ribeiro de Oliveira
Coordenação Técnica

Christina Aires Correa Lima
Fabiola Pasini Ribeiro de Oliveira
Julio Cesar Moreira Barbosa
Luisa Campos Faria
Equipe Técnica

Laura Schertel Mendes
Mônica Tiemy Fujimoto
Isabela Rosal Santos
Tayná Frota de Araújo
Coordenação Científica

DIRETORIA DE COMUNICAÇÃO – DIRCOM
Ana Maria Curado Matta
Diretora de Comunicação

Superintendência de Publicidade e Mídias Sociais
Mariana Caetano Flores Pinto
Superintendente de Publicidade e Mídias Sociais

Marcela Louise Moura Santana
Sarah de Oliveira Santana
Produção Editorial

DIRETORIA DE SERVIÇOS CORPORATIVOS – DSC
Fernando Augusto Trivellato
Diretor de Serviços Corporativos

Superintendência de Administração – SUPAD
Maurício Vasconcelos de Carvalho
Superintendente Administrativo

Alberto Nemoto Yamaguti
Normalização

Candeia Revisões/ Danúzia Queiroz
Revisão Gramatical

Editorar Multimídia
Projeto Gráfico e Diagramação

www.cni.com.br

/cnibrasil

@CNI_br

@cnibr

/cniweb

/company/cni-brasil

IEL
Instituto Euvaldo Lodi
PELO FUTURO DA INDÚSTRIA

SENAI
Serviço Nacional de Aprendizagem Industrial
PELO FUTURO DO TRABALHO

SESI
Serviço Social da Indústria
PELO FUTURO DO TRABALHO

CNI
Confederação Nacional da Indústria
PELO FUTURO DA INDÚSTRIA