IMPLEMENTAÇÃO E GESTÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Manual de orientações para a equipe e os colaboradores do IEPS

Versão revisada e atualizada

2023

Abreviaturas e acrônimos

2FA	*Two-Factor Authentication* (Autenticação de 2 Fatores)
ANPD	Autoridade Nacional de Proteção de Dados
CPF	Cadastro de Pessoa Física
DPO	*Data Protection Officer* (Encarregado de Proteção de Dados)
CEP	Comissão de Ética em Pesquisa
CONEP	Comitê Nacional de Ética em Pesquisa
GT	Grupo Técnico
IP	*Internet Protocol* (protocolo de internet)
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
NDA	*Non-disclosure agreement* (Acordo de Confidencialidade)
TCUD	Termos de Compartilhamento e Utilização de Dados
TI	Tecnologia da Informação
VPN	*Virtual Private Network* (Rede privada virtual)

Documento publicado em 02/10/2023 (vigência até 31/12/2024)

Sumário

Documento publicado em 02/10/2023 (vigência até 31/12/2024)

Glossário

Observação: este glossário não se propõe a ser exaustivo e inclui apenas as definições de termos mais relevantes para as discussões contidas neste documento. Definições adicionais sobre LGPD poderão ser encontradas na ***LEI Nº 13.709, DE 14 DE AGOSTO DE 2018*** *(Lei Geral de Proteção de Dados) e outros recursos.*

Agente de tratamento: o controlador e o operador.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

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

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 compete as decisões referentes ao tratamento de dados pessoais.

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

Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso, filosófico ou político; dado referente à saúde ou à vida sexual; dado genético ou biométrico, quando vinculado a uma pessoa natural.

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.

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

Encarregado (DPO): 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).

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome 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.

Pesquisa em Ciências Humanas e Sociais: aquelas que se voltam para o conhecimento, compreensão das condições, existência, vivência e saberes das pessoas e dos grupos, em suas relações sociais, institucionais, seus valores culturais, suas ordenações históricas e políticas e suas formas de subjetividade e comunicação, de forma direta ou indireta, incluindo as modalidades de pesquisa que envolvam intervenção (Resolução CONEP nº 510/2016).

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

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.

Introdução

Nos últimos anos, cresceu a preocupação com o tratamento de dados pessoais no mundo todo. Como resultado, normas e padrões foram desenvolvidos, a nível nacional e internacional, para aumentar a segurança e garantir a privacidade dos dados pessoais, sejam eles mantidos de forma física ou digital.

No Brasil, foi aprovada em agosto de 2018 a Lei Geral de Proteção de Dados (LGPD), que estabelece normas e sanções para garantir a proteção e segurança de dados de pessoas no território nacional. Como resultado, empresas e organizações passaram a adotar medidas para atender aos requisitos e às novas responsabilidades estipuladas pela Lei. Em 2021, o IEPS iniciou um processo de adequação à LGPD que incluiu o estabelecimento de novos protocolos, diretrizes e medidas para garantir a segurança de dados que estão ou venham a estar sob sua responsabilidade.

Este manual é um produto deste esforço. Tem como objetivo ser um material de referência e orientador para todos aqueles que, por qualquer razão, tenham contato com dados pessoais a partir de sua relação com o IEPS. O manual reúne as principais informações e orientações sobre a implementação de gestão da LGPD no instituto e conecta o leitor com recursos adicionais para apoiar o compartilhamento de conhecimentos e informações chave para o cumprimento da legislação. As diretrizes contidas neste manual e na Política Interna de Segurança da Informação se aplicam a qualquer meio, físico ou digital.

Esperamos que este manual sirva de apoio para todos os colaboradores do IEPS e que contribua para a boa governança e a segurança de dados no âmbito do Instituto. Como parte de um processo vivo e dinâmico, este documento será continuamente aprimorado e atualizado. Sugestões e contribuições para sua melhoria serão sempre bem-vindos. Agradecemos, desde já, a atenção e o cuidado de todos e todas às diretrizes aqui delineadas.

Documento publicado em 02/10/2023 (vigência até 31/12/2024)

O que é a LGPD?

A Lei Geral de Proteção de Dados (Lei nº 13.709), aprovada em agosto de 2018 e com vigência a partir de agosto de 2020, tem como objetivo estabelecer normas e práticas que garantam a proteção, dentro ou fora do país, de dados pessoais de pessoas que estejam no Brasil. A lei define dois tipos de dados que são sujeitos a cuidados específicos, porém diferenciados: dados pessoais, aqueles que permitem identificar uma pessoa viva, como CPF e RG; e dados sensíveis, que se referem a crianças e adolescentes e aqueles dados que revelem características específicas de uma pessoa (raça, etnia, dados de saúde, biometria, entre outros). A LGPD abarca tanto os dados tratados em meios físicos como digitais.

A LGPD deve ser cumprida independente da localização da sede da organização ou do centro de processamento ou armazenamento dos dados (seja em território nacional ou no exterior), desde que haja processamento de conteúdos relacionados a pessoas, brasileiras ou não, que estejam no território nacional.

Pontos importantes estabelecidos pela LGPD incluem:

- **Criação da Autoridade Nacional de Proteção de Dados (ANPD)**, responsável pela fiscalização e regulação da Lei; pessoas físicas e jurídicas estão sujeitas e devem responder à ANPD;
- **Estabelecimento de agentes de tratamento** com responsabilidades e funções na implementação da LGPD. Estes são os controladores (quem toma as decisões sobre o tratamento dos dados), o operador (quem realiza o tratamento dos dados) e o Encarregado (quem interage com as pessoas e a ANPD);
- **Consentimento** das pessoas como base para o tratamento dos seus dados pessoais e sensíveis. As situações em que a LGPD prevê exceções à necessidade de consentimento incluem: obrigação legal, execução de contratos, execução de política pública, preservação de integridade física e da vida, realização de ações por profissionais da saúde; prevenção de fraude, proteção ao crédito, e realização de estudos por órgão de pesquisa;
- **Garantias** às pessoas com relação ao tratamento e uso dos dados. Isso significa que as pessoas podem solicitar que seus dados sejam deletados ou transferidos, revogar consentimentos dados previamente, e solicitar a revisão de seus dados;
- **Gestão da implementação da LGPD**, o que significa que as organizações que administram dados pessoais passam a ter a obrigação de implementar normas de governança, medidas de segurança e boas práticas para garantir a segurança dos dados e o cumprimento da Lei.

Como o IEPS se organizou para implementar a LGPD?

Durante o ano de 2021, realizamos um processo minucioso de diagnóstico e adequação de procedimentos para assegurar a *compliance* do IEPS à nova Lei Geral de Proteção de Dados. O processo incluiu os seguintes passos:

- Contratação de consultoria jurídica para analisar o status atual de *compliance*;
- Realização de diagnóstico de infraestrutura de TI e adequações para melhoria de segurança de dados. Atualmente o IEPS atende aos requisitos definidos na LGPD;
- Mapeamento, revisão e adequação de contratos, protocolos, e procedimentos internos;
- Aprovação da Política Interna de Segurança de Dados pelo Conselho Deliberativo (novembro de 2021);
- Designação de Encarregado de Dado (DPO), conforme requer a Lei;
- Conformação de um grupo interno sobre segurança de dados (GT) responsável pela definição de protocolos internos e acompanhamento das ações de LGPD. Este grupo é composto por funcionários dos setores administrativo/financeiro, gestão, TI e equipes técnicas;
- Capacitação de DPO e do GT sobre a LGPD;
- Elaboração de documentos orientadores e sessões informativas sobre a LGPD para funcionários e colaboradores do IEPS.

A quem se aplicam estas orientações?

Este documento deve servir de referência a todos aqueles que têm qualquer nível de acesso a dados pessoais, confidenciais e/ou sensíveis que estão sob responsabilidade do IEPS. Inclui:

- Diretores e funcionários;
- Prestadores de serviço e fornecedores;
- Consultores;
- Estagiários;
- Bolsistas;
- Colaboradores e pesquisadores visitantes.

Documento publicado em 02/10/2023 (vigência até 31/12/2024)

Que tipos de dados o IEPS coleta e/ou armazena?

Área	Tipo de dados coletados/tratados	Como são coletados
Administrativo/ Financeiro	➢ Dados (pessoais e/ou sensíveis) de funcionários, parceiros, financiadores, colaboradores, fornecedores e candidatos em processos seletivos; ➢ Informações financeiras e contábeis do instituto e de parceiros.	➢ Contratos; ➢ Documentos admissionais; ➢ Documentos de processos seletivos; ➢ Atestados médicos; ➢ Formulários de medicina do trabalho; ➢ Dados de seguro saúde e de vida.
Gestão	➢ Dados biométricos do sistema de entrada nos escritórios.	➢ Cadastros biométricos de funcionários e visitantes aos escritórios.
Pesquisa	➢ Dados de bases públicas (ex. DataSUS) ou privadas (ex. CadÚnico); ➢ Dados pessoais e/ou sensíveis de participantes de pesquisas e projetos.	➢ DataSUS, Ministério da Cidadania, acordos com universidades, respostas a instrumentos de coleta de dados (questionários, entrevistas, etc.), pedidos da Lei de Acesso à Informação (LAI).
Políticas Públicas e Relações Institucionais	➢ Dados de bases públicas; ➢ Dados pessoais e/ou sensíveis de participantes de pesquisas e projetos.	➢ Respostas a instrumentos de coleta de dados (questionários, entrevistas, etc.), pedidos da Lei de Acesso à Informação (LAI).
Comunicação	➢ Nomes e e-mails coletados no site (cadastro da newsletter); ➢ Dados e imagens de colaboradores e convidados para eventos.	➢ Autorização de usuários do site; ➢ Termos de consentimento e uso de imagem de colaboradores e convidados de eventos.
TI	➢ Acesso secundário aos dados do instituto para proteção, backup e manutenção do sistema computacional; ➢ Dados pessoais (nome, telefone e endereço de e-mail); ➢ Informações técnicas dos equipamentos (IP).	Ver formas de coleta acima.

Como tratamos dados pessoais e sensíveis?

Local de armazenamento de dados	Quem são os responsáveis	Quem pode ter acesso
Google Drive	➢ Gerentes e supervisores das áreas.	➢ Funcionários com acesso autorizado; ➢ Parceiros com acesso autorizado (por ex. auditores e contadores); ➢ Fornecedores e prestadores de serviço com acesso autorizado.
Notebooks de trabalho	➢ Funcionários.	➢ Funcionários e equipe de TI.
NAS, servidor, backup na nuvem (AWS Glacier)	➢ Coordenadores e pesquisadores envolvidos; ➢ Equipe de TI.	➢ Coordenadores e pesquisadores envolvidos; ➢ Equipe de TI.
Sistema AlterData	➢ Administração.	➢ Equipe de Administração.
Mailchimp	➢ Equipes de Gestão e Comunicação.	➢ Funcionários com acesso autorizado.

Quais protocolos e medidas de segurança se aplicam aos dados no IEPS?

O IEPS se guia pela sua Política Interna de Segurança de Dados, em vigência desde novembro de 2021, que determina em seu Artigo 3, as normas e medidas que devem ser observadas para garantir a segurança dos dados.

Entre outras ações, destacamos:

Medidas de segurança na nuvem e servidor

Drive

Confira a seção “Manejo e cuidados necessários” para orientações detalhadas.

Documento publicado em 02/10/2023 (vigência até 31/12/2024)

NAS e Servidor

Para acesso ao NAS e servidor, é necessário que o colaborador preencha e assine o Termo de Confidencialidade e Proteção de Dados (NDA), instrumento que atesta a ciência quanto ao cumprimento das obrigações previstas na LGPD. A partir da assinatura, são definidos usuário e senha individual, com restrições de pastas definidas por nível de hierarquia de acesso, e utilização de certificado de segurança instalado no equipamento pela equipe da NASK. O acesso é feito via VPN, com configuração efetuada por meio do firewall Fortigate. A fim de aumentar o nível de proteção, é recomendada a ativação de Autenticação de 2 Fatores (2FA). As portas de segurança externas são fechadas, com acesso apenas utilizando IPs fornecidos pelo Fortigate; sem acesso à VPN, não é possível a conexão direta ao equipamento com IP público.

Microdados identificados são armazenados somente no servidor dedicado, desconectado da internet (offline), cujo acesso se dá por meio de um único terminal, com controle de acesso de usuários, ambos com rede própria (estilo “sala de sigilo”). O tratamento dos microdados identificados ocorre exclusivamente na máquina offline, e só poderão ser retirados da máquina mediante anonimização e autorização do responsável, que fará a verificação de que os dados foram tratados (anonimizados) adequadamente.

São feitas verificações de atualizações semanalmente, e, conforme necessidade, a manutenção é feita após horário comercial com aviso prévio aos usuários. A manutenção do sistema e arquivos é feita mensalmente com agendamento. Todos os atendimentos e procedimentos são realizados com ordem de serviços enviados para Helena Ciorra.

Protocolos de TI

Periodicamente, será feita uma varredura no Google Drive, NAS e servidor para exclusão de arquivos indevidos (por exemplo, arquivos pessoais armazenados erroneamente no Drive compartilhado) ou ociosos (sem nenhuma modificação) há mais de **1 ano**, com atenção a arquivos com indicação explícita de armazenamento de dados (por exemplo, arquivos de processos seletivos como CVs), exceto se indicado pelo responsável do arquivo, pasta ou projeto.

Além disso, anualmente ocorre a manutenção preventiva das máquinas institucionais utilizadas pelos colaboradores, agendada diretamente de forma escalonada. Trata-se de um acesso aos equipamentos que utilizam para acessar a infraestrutura do IEPS, verificando-se o nível de segurança dos equipamentos, passando por questões como atualizações, arquivos maliciosos e possíveis defeitos que possam comprometer o trabalho.

Ademais, todas as redes são protegidas por *firewall*, todas as máquinas têm antivírus instalado e monitoramento da equipe de TI.

Implementação de instrumentos e termos de autorização específicas para garantir adequação à LGPD

- ★ Termos de consentimento de uso de imagem, para a utilização de imagem de colaboradores e parceiros em publicações, Diálogos IEPS, relatórios, sites, entre outros;
- ★ *Non-disclosure agreement* (NDA) para pesquisadores, funcionários, colaboradores, bolsistas e estagiários que têm acesso a bases de dados que estão sob responsabilidade do IEPS ou de colaboradores do IEPS;
- ★ Política de privacidade para os sites do IEPS (link incluído em todos os sites);
- ★ Termo de consentimento para tratamento de dados pessoais de empregados em regime CLT (aditivo a contratos de trabalho);
- ★ Cláusulas específicas sobre LGPD, sigilo e confidencialidade em contratos com prestadores de serviço, consultores e parceiros;
- ★ Termos de compartilhamento e utilização de dados (TCUD) para acesso a bases de dados restritas ou identificáveis (assinadas com universidades, órgãos públicos ou privados responsáveis por bases de dados de interesse ao IEPS).

Para acesso aos modelos utilizados, ver a seção "Recursos Adicionais" ou, para mais informações, a seção "Contato para dúvidas, orientações e comunicações de problemas".

Manejo e cuidados necessários no tratamento dos dados

Drive

Organização

Procure manter nosso Drive organizado. Não crie pastas fora da sua área ("Comunicação", "Gestão", "Pesquisa" etc.), e mantenha coerência nos caminhos, nomeando os arquivos e pastas de forma clara e objetiva. Isso evitará a exclusão equivocada de arquivos importantes.

Mesmo que faça sentido naquele momento (devido à facilidade de acesso), evite manter arquivos duplicados em diversas pastas. Além de consumir espaço, isso abre margem para

armazenamento indevido de dados devido ao esquecimento de cópias. Caso tenha dúvidas sobre onde armazenar algo, entre em contato com Helena Ciorra .

Processos Seletivos

Todos os novos processos seletivos serão criados e gerenciados dentro de pasta específica na área de Gestão Institucional, com acesso restrito às equipes de Administração e Gestão e liberação manual de acesso a membros relevantes das equipes (por exemplo, se for uma vaga da área de Políticas Públicas, será concedido acesso, a um ou dois membros desta equipe, à pasta com CVs e demais documentos). Isso é necessário para garantir que materiais submetidos ao IEPS, como parte de candidaturas a vagas abertas, e que contém dados pessoais dos candidatos estejam devidamente protegidos.

Nenhum colaborador deve criar pastas de processos seletivos por conta própria. Peça auxílio a alguém da equipe de Gestão ou Administração (Helena Ciorra ou Rodrigo Soares).

Para os formulários de inscrição em processos seletivos, recomendamos que este já inclua perguntas que informem o candidato sobre **1)** o tratamento de seus dados para o processo seletivo em questão; **2)** o possível armazenamento de seus dados no Banco de Talentos. É importante frisar que a mera inclusão da pergunta não isenta da confirmação, junto ao candidato, de que ele consente com a coleta e tratamento de seus dados para esta finalidade.

Confira o manual de Orientações para Processos Seletivos para mais informações sobre o fluxo adequado, disponível também na intranet.

Caso haja interesse em manter o currículo de um candidato para compor o Banco de Talentos, o faça **apenas após coletar o consentimento inequívoco do candidato**. Em seguida, envie as informações ao ponto focal de sua equipe ou diretamente à equipe de Gestão. Os documentos devem ser armazenados exclusivamente na pasta compartilhada “Banco de Talentos IEPS”, cujo acesso é controlado e restrito. Os currículos não devem ser salvos em discos locais de computadores (pessoal ou profissional) nem em Drives pessoais dos colaboradores.

Confira o Guia de Orientações para composição do Banco de Talentos IEPS para mais informações.

Controle de acesso a pastas e documentos

Ao criar um documento novo no Drive , atente-se para dois detalhes importantes:

1. **Ele foi criado na pasta apropriada?**

Documentos colaborativos e/ou públicos (texto de divulgação de algum material, roteiro de algum evento etc.) devem ser criados **DENTRO** da pasta compartilhada **IEPS Oficial**, na sub-pasta apropriada (Comunicação, Gestão etc. O caminho a partir daqui fica a critério do usuário, porém pedimos manter coerência na criação de pastas).

2. **Ele é um arquivo de acesso restrito?**

   Todos os arquivos dentro de um "Drive compartilhado" (caso do "IEPS Oficial") são visíveis para todos os colaboradores da pasta. Se seu arquivo trata-se de um documento com dados sensíveis, orientamos que arquive ele em seu Drive pessoal e compartilhe apenas com as pessoas apropriadas.

   Caso deseje disponibilizá-lo dentro do Drive compartilhado, para facilitar a organização, basta criar um atalho dentro do diretório apropriado.

   Faça periodicamente a checagem das permissões vigentes em pastas e arquivos e, caso identifique algum material sensível que não deve ser compartilhado, entre em contato com Helena Ciorra **para gerenciamento.**

Celulares e outros dispositivos móveis

O uso do WhatsApp como ferramenta de comunicação faz parte do nosso dia a dia e é inclusive utilizado como estratégia de gestão e engajamento em nossos projetos e parcerias. Por isso, é necessário ter em mente algumas precauções na utilização deste e outros aplicativos em dispositivos móveis, buscando sempre a adoção de medidas de segurança e melhores práticas na coleta e tratamento de dados:

- **Finalidade/legitimidade do tratamento de dados pessoais**: a transmissão de dados pessoais por WhatsApp ou outros aplicativos deve sempre ser devidamente justificada;
- **Eliminação de dados pessoais contidos nos grupos de WhatsApp**, quando não se justifica mais manter os dados armazenados;
- **Consentimento dos titulares** caso haja utilização ou tratamento de dados pessoais para além da comunicação dentro do aplicativo, sempre considerando as hipóteses definidas pela Lei nas quais o consentimento é necessário;
- **Respaldo em contrato** no caso de compartilhamento dos dados pessoais com outras instituições, incluindo os parceiros dos projetos.

Computador pessoal

Como a maioria das máquinas cedidas pelo IEPS aos colaboradores é registrada sob o mesmo login, é possível que a opção de **Compartilhamento entre dispositivos** esteja ativada, pois este é o padrão de fábrica. Isso fará com que seus arquivos "apareçam" no computador de outro colaborador, ou que os arquivos de outras pessoas apareçam no seu, o que pode acarretar o compartilhamento de arquivos sensíveis. **Desative essa opção o quanto antes.** Caso precise de suporte, entre em contato com o Encarregado (DPO).

Backups

Procure sempre fazer cópias de segurança de arquivos importantes e armazená-los em locais diferentes dos arquivos originais (se o arquivo original está na nuvem, faça um backup local em seu HD, e vice-versa), assim ele não corre os mesmos riscos de perda ou dano. Para isso, crie uma pasta com indicação clara do que se trata ("Backup", "Arquivo" etc.).

Antes de criar cópias físicas (CDs, DVDs, pendrives) de qualquer tipo de arquivo, consulte o Encarregado (DPO).

Lembre-se de que todas as orientações e medidas de segurança deste manual também se aplicam aos backups, pois estes podem conter documentos com dados pessoais e sensíveis.

Responsabilidades do IEPS

A LGPD instituiu um regime jurídico especial mais flexível para o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Os **art. 7** e **11** da LGPD preveem que o tratamento de dados por órgãos de pesquisa é uma das modalidades que prescinde de consentimento do titular. Porém, isso não significa que não devem ser levadas em conta uma série de providências e medidas protetivas para que essa pesquisa ocorra regularmente.

Mesmo o tratamento de dados pessoais cujo acesso seja público também deve observar a LGPD. Mais especificamente, o tratamento desses dados pessoais deve se amparar em uma hipótese legal apropriada e respeitar "a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização", resguardados os direitos dos titulares.

Assim, é de responsabilidade do IEPS garantir um ambiente seguro para o tratamento adequado dos dados pessoais sob sua custódia, por meio de redes seguras e controladas,

garantindo a anonimização ou pseudonimização dos dados sempre que possível e sendo vedada a sua transferência a terceiros.

O tratamento de dados pessoais para fins administrativos ou comerciais, ainda que possua algum vínculo indireto com ações de pesquisa, deve respeitar **integralmente** a LGPD. É o caso da coleta de dados pessoais para realização de contratos, processos seletivos, ou tratamento de dados de funcionários pelo setor de recursos humanos da instituição.

Aplica-se integralmente a LGPD também em coletas de dados pessoais realizados durante atividades como oficinas com gestores, por exemplo. Nestes casos, além do consentimento inequívoco do titular para a coleta e tratamento de seus dados, é necessária a assinatura de termo de consentimento caso haja também coleta de imagens.

Em caso de dúvida se o tratamento de dados pessoais se enquadra na exceção para atividades acadêmicas, **recomendamos optar sempre por atender às disposições pertinentes da LGPD** ("pecar pelo excesso").

Direitos e condutas esperadas dos colaboradores

Espera-se que os colaboradores se mantenham atualizados por meio da leitura da Lei Geral de Proteção de Dados Pessoais (LGPD) e deste manual a respeito de instruções, normas e políticas institucionais pertinentes às atividades do IEPS, aplicando-as no exercício de suas funções. O que **não** significa que qualquer colaborador do IEPS deva responder diretamente às demandas de informações embasadas nas previsões da LGPD. Caso você receba alguma solicitação, oriente que o contato seja feito via e-mail do Encarregado (dpo@ieps.org.br, disponível também na Política de Privacidade).

Desta forma, os colaboradores contribuirão, de maneira bem informada e consciente, com o correto atendimento das previsões contidas na Lei e manterão uma postura de respeito à gestão da privacidade e à proteção de dados pessoais.

Não envie ou compartilhe quaisquer dados com terceiros (parceiros ou não) sem consulta e autorização prévia do IEPS, bem como não colete mais dados do que aqueles que sejam realmente necessários para realizar a atividade pretendida.

Todos os colaboradores devem atentar-se para as orientações presentes no Código de Ética e nas Diretrizes Internas e Boas Práticas em Pesquisa.

Por fim, espera-se que qualquer colaborador comunique ao Encarregado suspeitas ou eventos que violem a Política Interna de Segurança da Informação ou que possam colocar em risco os dados pessoais sob a gestão do IEPS.

Documento publicado em 02/10/2023 (vigência até 31/12/2024)

Orientações sobre o tratamento dos dados uma vez coletados

Se os dados coletados tratarem-se de microdados/bases de dados cujo tratamento exclusivo é relacionado a atividades de pesquisa, estes devem ser armazenados no servidor do IEPS, seguindo as orientações para correta identificação.

Caso tratem-se de dados coletados para quaisquer outros fins que não de pesquisa, eles devem ser armazenados em pastas restritas, com controle de acesso. Após realizar a coleta, recomendamos que organize-os de acordo com a planilha-modelo fornecida, dando conta de todos os dados coletados, a fim de ajudar no controle interno. Dados oriundos de processos seletivos podem ser organizados conforme planilha própria do formulário original. As planilhas também devem ter acesso restrito e controlado, e não devem ser feitas cópias para locais de armazenamento pessoais. **Defina claramente quem pode ter acesso a estes dados, quais as finalidades de tratamento e o período total do tratamento**. Em seguida, informe e envie sua planilha de dados ao Encarregado (DPO), que fará o controle da coleta em uma planilha dedicada.

Quais são os riscos de vazamento de dados e o plano de contingência caso isso ocorra?

Apesar de todos os cuidados e precauções, sempre existe o risco de vazamentos de dados. Os fatores que podem contribuir para estas situações incluem: erro humano, hackeamento e desconfiguração do Drive.

Caso se identifiquem situações de risco à integridade de dados ou algum vazamento de dados, os seguintes passos deverão ser seguidos:

- Comunicar imediatamente aos Encarregado (DPO), supervisores diretos e ao GT de Segurança de Dados;
- O Encarregado e o GT comunicarão imediatamente à Diretoria qualquer vazamento ou situação que comprometa a integridade de dados sob responsabilidade do IEPS;
- Caso haja vazamento de dados pessoais e/ou sensíveis, os titulares dos dados também serão comunicados pelos Encarregado;
- A partir da análise da situação, o Encarregado e o GT poderão realizar as seguintes ações adicionais:
    - Acionar a assessoria de TI para diagnóstico e correção do problema;

- Acionar a assessoria jurídica para aconselhamento e encaminhamentos jurídicos necessários.

LGPD e ética em pesquisa: o que precisamos saber?

Pesquisas que envolvem seres humanos, como as que ocorrem nas áreas da saúde, ciências humanas e sociais, com frequência envolvem a coleta e processamento de dados pessoais e sensíveis, como, por exemplo, registros de mortalidade e médicos, dados populacionais, dados de utilização de serviços, entre outros.

No Brasil, o sistema CEP/CONEP institui e regula as normas e diretrizes relacionadas à garantia dos princípios éticos e à proteção dos participantes das pesquisas que envolvem seres humanos. Isso se realiza através de normativas e resoluções publicadas pelo Conselho Nacional de Saúde (ver seção "Recursos Adicionais").

Um aspecto importante das ações do sistema CEP/CONEP está relacionado à proteção de dados pessoais e sensíveis coletados de participantes de pesquisas (por ex. a normatização sobre questões de sigilo e confidencialidade). Neste sentido, a LGPD significou um avanço ao dar caráter legal e fortalecer as normas já estabelecidas anteriormente pelas resoluções do CEP/CONEP.

A LGPD, como uma lei geral, é voltada ao estabelecimento de princípios e diretrizes norteadores para proteger os direitos dos titulares de dados e, ao mesmo tempo, permitir o processamento de dados pessoais e sensíveis para fins determinados, como por exemplo, a pesquisa científica e a execução de políticas públicas. Porém, com a sua aprovação, questões referentes à ética em pesquisa podem parecer ter dupla normatização, uma vez que as orientações da Lei e as Resoluções do CEP/CONEP nem sempre estão alinhadas.

Os marcos regulatórios e novas normativas ainda estão em desenvolvimento e devem ser considerados em consonância com as normas específicas dos setores envolvidos (por ex. as normas do setor saúde). Em linhas gerais, questões de ética em pesquisa que envolve seres humanos são reguladas pelo sistema CEP/CONEP, enquanto as questões de legalidade do processamento de dados pessoais e sensíveis são reguladas pela LGPD.

A LGPD traz as seguintes implicações para o uso de dados em pesquisa:

- Define as condições para o uso de dados pessoais, entre os quais a utilização por órgãos de pesquisa, como o IEPS, desde que seja garantida, sempre que possível, a anonimização;
- A normatização sobre o uso de dados sensíveis, o que é permitido apenas com o consentimento específico do titular. Há, porém, a exceção para o seu uso na realização de estudos por órgãos de pesquisa, desde que seja garantida, sempre que possível, a anonimização (ver seção "Perguntas Frequentes");
- A exigência de que os responsáveis pelo tratamento de dados pessoais organizem e mantenham registros cuidadosos acerca de qualquer atividade relacionada ao processamento de dados sob sua responsabilidade, garantindo que o titular dos dados possa ter acesso e solicitar ações sobre os mesmos (por exemplo, solicitar sua eliminação e alteração, ou retirar o consentimento).

Com relação às pesquisas e projetos realizados pelo IEPS que incluam coleta ou tratamento de dados de seres humanos, as recomendações no momento são:

- Definir procedimentos claros de coleta e processamento dos dados pessoais e sensíveis, considerando: a base legal para a utilização dos dados; as medidas de segurança apropriadas; o uso dos dados apenas para a finalidade da atividade, estudo ou projeto; e a aprovação ética do protocolo do estudo ou projeto, quando aplicável;
- Descrever claramente nos Termo de Consentimento Livre e Esclarecido (TCLE), quais são os protocolos de utilização e armazenamento dos dados. Nos casos em que há base para solicitar dispensa do TCLE junto ao Sistema CEP/CONEP, esta deve descrever como os pesquisadores se comprometem a mitigar riscos e assegurar os direitos dos participantes, incluindo as questões de confidencialidade, privacidade dos titulares dos dados, proteção de imagem e cuidados para a não estigmatização de indivíduos e grupos;
- Atentar às orientações sobre os locais físicos e virtuais para o armazenamento e processamento dos dados e os protocolos de segurança para garantir que estes se mantenham protegidos, de acordo com a nossa Política Interna de Segurança de Dados;
- Restringir ao máximo as possibilidades de identificação ou re-identificação de indivíduos ou o uso não autorizado dos dados. Por exemplo, pesquisas e projetos devem ser muito criteriosos sobre quais dados são realmente necessários coletar para a análise ou projeto em questão e assegurar que todas as pessoas que tenham acesso aos dados assinem os termos aplicáveis;
- Implementar medidas e acordos que restrinjam acesso aos dados apenas às pessoas da equipe ou colaboradores que devem ter esse acesso (por exemplo,

Termos de Compartilhamento e Utilização de Dados, Termos de Responsabilidade, NDAs, entre outros);

- Definir processos seguros de transferência de dados e, se for necessário, manter dados fora da internet e com acesso restrito;
- Acompanhar de perto as atividades de divulgação de resultados e os produtos resultantes de projeto para garantir que estes estão de acordo com as normas estabelecidas e a Política Interna de Segurança de Dados (por exemplo, assegurar que dados pessoais ou sensíveis, ou imagens, não sejam utilizados sem o devido consentimento).

Contatos para dúvidas, orientações e comunicações de problemas

- Encarregado de dados (DPO)
  - ➔ Helena Ciorra: dpo@ieps.org.br

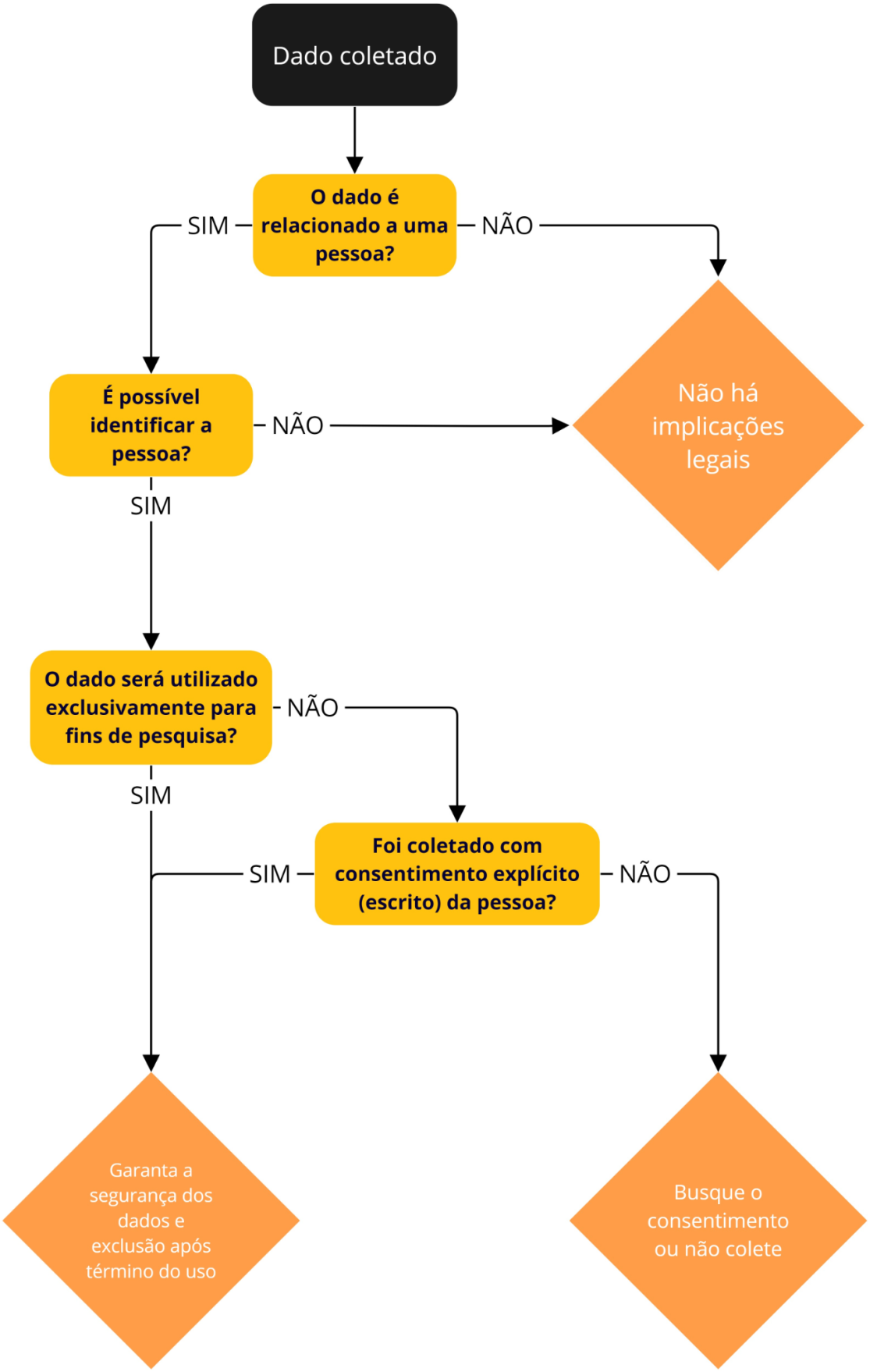
- GT de Segurança de Dados
  - ❖ Questões relacionadas ao setor administrativo, recursos humanos e financeiro:
    - ➔ Thaisa Marques: thaisa.marques@ieps.org.br
    - ➔ Rodrigo Soares: rodrigo.soares@ieps.org.br
  - ❖ Questões relacionadas a pesquisas, instrumentos e protocolos:
    - ➔ Maria Cristina Franceschini: cristina.franceschini@ieps.org.br
    - ➔ Beatriz Almeida: beatriz.almeida@ieps.org.br
    - ➔ Helena Ciorra: helena.ciorra@ieps.org.br
  - ❖ Questões relacionadas a TI:
    - ➔ Helena Ciorra: helena.ciorra@ieps.org.br

- Assessoria Jurídica
  - ➔ Contato institucional através de cristina.franceschini@ieps.org.br

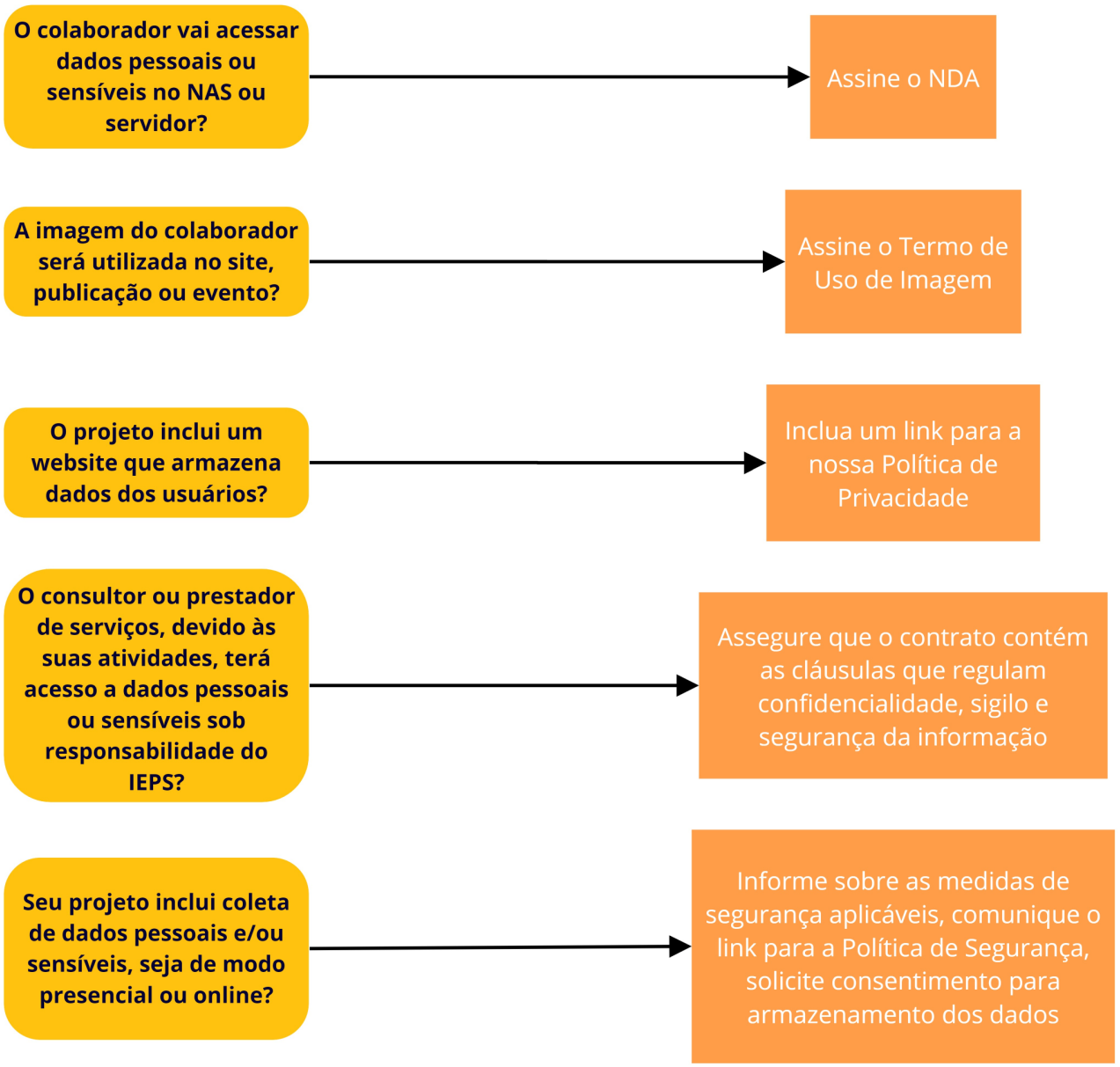
- Assessoria técnica de TI
  - ➔ NASK Assessoria em Informática: ti@ieps.org.br

- Ouvidoria do IEPS
  - ➔ Formulário
  - ➔ ouvidoria@ieps.org.br

Fluxogramas



Documento publicado em 02/10/2023 (vigência até 31/12/2024)


O colaborador vai acessar dados pessoais ou sensíveis no NAS ou servidor?
Assine o NDA
A imagem do colaborador será utilizada no site, publicação ou evento?
Assine o Termo de Uso de Imagem
O projeto inclui um website que armazena dados dos usuários?
Inclua um link para a nossa Política de Privacidade
O consultor ou prestador de serviços, devido às suas atividades, terá acesso a dados pessoais ou sensíveis sob responsabilidade do IEPS?
Assegure que o contrato contém as cláusulas que regulam confidencialidade, sigilo e segurança da informação
Seu projeto inclui coleta de dados pessoais e/ou sensíveis, seja de modo presencial ou online?
Informe sobre as medidas de segurança aplicáveis, comunique o link para a Política de Segurança, solicite consentimento para armazenamento dos dados

Perguntas frequentes

1. **As questões de LGPD e ética em pesquisa se aplicam a quais atividades do IEPS?**

   Para fins da LGPD, o IEPS é um "órgão de pesquisa", considerando a seguinte definição contida no Artigo XVIII:

   > *"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".*

   Como órgão de pesquisa, o IEPS responde também às resoluções do CONEP. A Resolução nº 510/2016 define "pesquisa em ciências humanas e sociais" como sendo "aquelas que se voltam para o conhecimento, compreensão das condições, existência, vivência e saberes das pessoas e dos grupos, em suas relações sociais, institucionais, seus valores culturais, suas ordenações históricas e políticas e suas formas de subjetividade e comunicação, de forma direta ou indireta, incluindo as modalidades de pesquisa que envolvam intervenção".

   Desta forma, as orientações relativas à LGPD e ética e pesquisa se aplicam a todos os projetos do IEPS, sejam eles realizados pela equipe de pesquisa ou de políticas públicas, desde que suas atividades incluam "procedimentos metodológicos que envolvam a utilização de dados diretamente obtidos com participantes e/ou de informações identificáveis ou que possam acarretar riscos maiores do que os existentes na vida cotidiana." Neste grupo se incluem pesquisas, atividades e projetos que utilizem métodos de coleta de dados como enquetes, entrevistas, grupos focais, consultas online, bases de dados com informações restritas ou identificáveis, entre outros.

2. **Qual tratamento o IEPS dá a dados biométricos?**

   O IEPS coleta dados pessoais biométricos em duas situações: (1) cadastro de funcionários para acesso ao escritório e controle de jornadas e (2) cadastro de visitantes que acessam as instalações do IEPS. O controle de jornada através de biometria é justificável por força do art. 11, II, "a", da Lei 13.709/18 (LGPD), entendendo-se esse tratamento de dados sensíveis como "cumprimento de obrigação legal ou regulatória pelo controlador", dispensando o consentimento específico. No caso do visitante, trata-se de medida de segurança, necessária à "proteção da vida ou da incolumidade física do titular ou de terceiro", na forma do

art. 11, II, “e”, da mesma lei. Sendo assim justificável, dispensa o consentimento específico. O tratamento e armazenamento desses dados sensíveis (onde, por quanto tempo, dispondo acesso a quem, como, sob quais sistemas de proteção etc) é regulamentado pelos itens 3.1.2 e 3.1.2.1. da Política Interna de Segurança de Dados.

3. **A LGPD tem previsões específicas para órgãos de pesquisa ou de terceiro setor, com fins não-econômicos, como o IEPS?**

   A Resolução CD/ANPD nº. 2 de 27 de janeiro de 2022 define um regime especial de tratamento de dados pessoais por agentes de pequeno porte. Esta inclui algumas provisões como: maior prazo para atender solicitações dos titulares sobre o tratamento de seus dados pessoais e para comunicar a ocorrência de incidente de segurança que não houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional; dispensa do Encarregado de dados (DPO), ainda que remanesça o dever de indicar um canal de comunicação. Sendo, no entanto, a designação de um DPO uma reconhecida boa prática, necessária para garantir um ambiente e uma cultura de segurança da informação nas organizações, o IEPS optou por manter esta função.

4. **Dados usados em pesquisas nem sempre são coletados pelo IEPS, então não nos cobrimos com a base legal do consentimento, pelo menos não diretamente. Então, nosso tratamento de dados pessoais seria legitimado como “realização de estudos por órgãos de pesquisa” e “execução de políticas públicas”?**

   Para fins da LGPD, o IEPS é um “órgão de pesquisa”, considerando a seguinte definição contida no Artigo XVIII:

   > *“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”.*

   Enquanto “órgão de pesquisa”, o IEPS está coberto sob algumas normas que favorecem e facilitam o desenvolvimento de pesquisas. A “realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais” é uma das situações enumeradas pela lei que legitima o tratamento de dados pessoais (inclusive dados sensíveis) de forma direta, ou seja, sem consentimento, nos termos do art. 7º, IV e 11, II, “c”. Há, ainda, na LGPD, uma

norma que importa particularmente ao perfil de atuação do IEPS, que é o art. 13, que disciplina a realização de estudos em saúde pública:

> *Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.*
>
> *§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.*
>
> *§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.*
>
> *§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.*
>
> *§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.*

Por fim, há ainda uma prerrogativa especial, de conservação de dados pessoais resultantes de pesquisa nas seguintes finalidades quando necessários para "estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais" (art. 16).

5. **Qual tratamento deve ser dado às bases que contém dados pessoais e que são utilizadas para pesquisas no IEPS, incluindo dados obtidos através de Leis de Acesso à Informação (LAI) e pelo Portal de Transparência?**

Em se tratando de dados pessoais necessários à realização de pesquisa, os parâmetros descritos na resposta às perguntas 3 e 4 são aplicáveis. Embora não deixem de ser dados pessoais, são utilizados para finalidade legítima e, afinal, são públicos. Os cuidados aplicáveis são os mesmos mencionados antes, devendo se

observar, em especial, a finalidade, a boa-fé e interesse público que justificaram sua disponibilização (art. 7º, § 3º).

6. **Na realização de um projeto, o IEPS receberá dados de órgão público, como as Secretarias de Saúde. Há alguma cautela que devemos tomar?**

   Além dos cuidados descritos na resposta às perguntas 3, 4 e 5, é imprescindível que a transferência de dados esteja prevista em um instrumento contratual celebrado entre o IEPS e o órgão público. Isso pode ocorrer com a inclusão de uma cláusula de proteção de dados pessoais no acordo de cooperação ou mesmo mediante a assinatura de um termo de proteção a dados pessoais apartado, quer exista ou não acordo cooperação já assinado. A LGPD trata a transferência de dados pessoais do Poder Público para particulares como excepcional e, nesses casos, ela somente poderá ocorrer mediante a previsão expressa em instrumento contratual, por exigência do art. 26, IV.

   Ademais, aplicam-se as orientações padrão sobre armazenamento seguro dos dados no servidor (e no servidor offline, caso tratem-se de dados identificados). Todo o procedimento deve ser realizado sob supervisão do Encarregado de Dados (Helena Ciorra) e da equipe de TI (Nask).

7. **Em um projeto, os dados pessoais foram coletados informando uma determinada finalidade ao titular de dados. O IEPS deseja, agora, utilizar este dado para finalidade ligeiramente distinta. É possível ou deve-se obter novo consentimento do titular de dados?**

   É permitido o tratamento de dados pessoais para uma atividade distinta daquela que justificou sua coleta, em momento inicial. Neste caso, é imprescindível que esse tratamento posterior seja compatível com as finalidades do tratamento original.

   Na realização de pesquisas, há uma presunção de compatibilidade entre os propósitos secundários e a finalidade original do tratamento de dados. Isso não dispensa a demonstração de que o tratamento dos dados para a nova finalidade possui propósitos legítimos e que guarde compatibilidade com a finalidade original informada ao titular de dados.

   Deve-se levar em conta, ainda, (i) a natureza dos dados pessoais, adotando-se cautelas maiores quando dados sensíveis estiverem envolvidos; (ii) as expectativas legítimas dos titulares de dados e potenciais impactos do tratamento posterior sobre seus direitos; (iii) a adoção de medidas de segurança e prevenção apropriadas e (iv) as exigências de ética em pesquisa eventualmente aplicáveis ao caso.

8. **O IEPS pode indeferir pedidos de exclusão de titulares de dados quando precisar armazená-los para os propósitos de suas pesquisas?**

   Caso o IEPS receba o pedido de exclusão dos dados pessoais do titular de dados, mas seja imprescindível, para os propósitos da pesquisa, armazenar esses dados, o IEPS poderá indeferir a solicitação do titular dos dados e mantê-los armazenados.

   Essa eventual negativa deve sempre ser motivada, demonstrando que a manutenção dos dados pessoais é medida necessária e possui um vínculo real com o atendimento à finalidade específica da pesquisa.

   Sempre que possível, os dados deverão ser anonimizados e excluídos após a realização das atividades que levaram à sua coleta.

9. **Quais são as regras relacionadas à vigência da LGPD e as irregularidades previstas na Lei?**

   As sanções começam a ser aplicadas sobre fatos ocorridos a partir de agosto de 2021, conforme regra da Lei 13.709/18 (art. 65, I, "a"). A constatação de uma infração pode ocorrer por diferentes meios, desde a reclamação de um titular até um processo de monitoramento da ANPD. Constatando-se o fato, inicia-se um processo de apuração regido por uma Resolução específica da ANPD.

   A regra sobre prescrição é: "Prescreve em cinco anos a ação punitiva da Administração Pública Federal, direta e indireta, no exercício do poder de polícia, objetivando apurar infração à legislação em vigor, contados da data da prática do ato ou, no caso de infração permanente ou continuada, do dia em que tiver cessado" (art. 1º, Lei 9.873/99). Neste contexto, o "poder de polícia" diz respeito a qualquer modalidade de fiscalização, incluindo aquela que é promovida pela Autoridade Nacional de Proteção de Dados. Assim, a ANPD tem o prazo de 5 anos para iniciar a apuração sobre uma conduta que viole a LGPD, a contar da data em que ocorreu o fato ilícito (se foi em apenas um dia) ou do dia em que tiver cessado (se a conduta foi contínua). Durante os 5 anos, pode haver suspensão ou interrupção do prazo, assim como encerramento do processo, caso ele permaneça paralisado por mais de 3 anos.

10. **Em caso de irregularidades, como se aplicam as sanções administrativas previstas na LGPD?**

    O processo sancionatório é sempre graduado em função de determinados fatores, como a gravidade da conduta irregular, e outros (alguns enumerados pela lei). A tendência é o escalonamento, ou seja, começando pela sanção mais leve e (conforme a reincidência, por exemplo), chegando às mais gravosas. É cabível,

porém, a celebração de termo de ajustamento de conduta, que afasta ou reduz a imposição de sanções, conforme resolução da ANPD.

11. **Todos os formulários devem conter alguma menção à LGPD?**

Sim. Caso trate-se de uma atividade de pesquisa, não é necessário que o IEPS obtenha o consentimento direto das pessoas envolvidas na coleta. Porém, mesmo tratando-se de uma pesquisa ou até mesmo um tipo de colaboração mais técnica (desenvolvimento de políticas públicas), o art. 6, V e VI fala sobre a necessidade de conferir clareza no tratamento dos dados pessoais do titular. Então é uma boa prática assegurar a clareza e transparência na coleta de qualquer dado.

12. **É preciso sempre explicitar o que será feito com os dados coletados?**

Sim. Mesmo que os art. 7 e 11 respaldem a coleta sem consentimento no caso da finalidade ser para pesquisa, a boa prática dita que seja explicitado o alcance daquela coleta.

13. **Durante a realização de oficinas, quais os pontos de atenção a serem observados na coleta de dados de participantes?**

Oficinas e formações não se enquadram como atividade de pesquisa prevista no art. 7, tampouco no art. 26. Por isso, é preciso ter um cuidado especial na coleta e no gerenciamento de quaisquer dados coletados durante estes eventos, principalmente tratando-se de registros fotográficos. Para toda coleta e uso de imagem é imprescindível o consentimento inequívoco do titular. Este consentimento pode ser obtido por meio de termo específico ou por meio de aceite inequívoco durante formulário de inscrição para qualquer atividade, onde deve estar explícita a finalidade e tratamentos a serem realizados. Antes de utilizar a imagem de qualquer participante, deve-se confirmar que as pessoas específicas presentes no registro fotográfico consentiram com o tratamento de seus dados para esta finalidade.

14. **Posso guardar um CV que me interessou, que foi coletado em algum processo seletivo ou que recebi por e-mail diretamente da pessoa?**

O IEPS tem um Banco de Talentos, para armazenar candidaturas de interesse que eventualmente não foram selecionadas em processos seletivos. Caso queira indicar um candidato para compor o Banco de Talentos, o faça apenas após coletar o consentimento explícito do candidato via e-mail, informando a finalidade do tratamento e período que será armazenado. É necessário que o colaborador do IEPS que realizar a coleta do currículo guarde também todo o registro de comunicação com o candidato, que comprova o consentimento para o tratamento

dos dados durante o período estabelecido. Em seguida, informe seu coordenador e o ponto focal de sua equipe; eles deverão informar o Encarregado (DPO) sobre o armazenamento dos documentos, que ocorrerá exclusivamente na pasta compartilhada “Banco de Talentos IEPS”, cujo acesso é controlado e restrito. Os currículos não devem ser salvos em discos locais de computadores (pessoal ou profissional) nem em Drives pessoais dos colaboradores.

Entendemos que currículos que chegam de forma espontânea diretamente pelos canais de comunicação do IEPS (como e-mails) carregam o consentimento implícito do candidato para o tratamento dos dados nesta finalidade.

15. Como posso acessar os microdados sob responsabilidade do IEPS, armazenados no servidor?

Existem formalidades que devem ser observadas durante o tratamento de dados, em especial a correta identificação das pessoas autorizadas a ter acesso a dados pessoais e para a condução de estudos e pesquisas. Para tanto, o IEPS utiliza um Termo de Confidencialidade (NDA) como instrumento para atestar a ciência do colaborador quanto à realização do estudo e ao cumprimento das obrigações pertinentes previstas na LGPD. Entre estas obrigações, destaca-se a vinculação do uso dos dados à finalidade exclusiva de realização do estudo e o compromisso de respeitar a confidencialidade dos dados e a privacidade dos titulares e de adotar as medidas de prevenção e segurança apropriadas ao caso. Para solicitar o acesso ao servidor e assinatura do NDA, entre em contato com o Encarregado (DPO).

Recursos adicionais

★ IEPS - Política Interna de Segurança de Dados

★ IEPS - NDA para pesquisadores

★ IEPS - Termo de consentimento de uso de imagem

★ IEPS - Política de Privacidade para sites

★ ANPD - Guia Orientativo sobre o Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas

★ LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados -

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

★ Curso Introdutório gratuito sobre LGPD - Fundamentos da Lei Geral de Proteção de Dados (Carga horária: 10h)

https://www.escolavirtual.gov.br/curso/603

★ Carta Circular 1/2021-CONEP/SECNS/MS. Orientações para procedimentos em pesquisas com qualquer etapa em ambiente virtual.

http://conselho.saude.gov.br/images/comissoes/conep/documentos/CARTAS/Carta_Circular_01.2021.pdf

★ Política de gestão, compartilhamento e abertura de dados para pesquisa: Princípios e Diretrizes (documento da Fiocruz para referência às suas pesquisas mas com informações relevantes e aplicáveis a outras pesquisas)

https://www.arca.fiocruz.br/bitstream/icict/46408/2/VPEIC_versao_PORTUGUES_2021-03-22.pdf

★ Research Data Alliance (rede mundial de pesquisadores que discutem questões relacionadas ao uso e compartilhamento de dados)

https://www.rd-alliance.org/

★ RESOLUÇÃO Nº 466, DE 12 DE DEZEMBRO DE 2012. Diretrizes e Normas Regulamentadoras de Pesquisas envolvendo Seres Humanos.

https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf

Documento publicado em 02/10/2023 (vigência até 31/12/2024)

★ RESOLUÇÃO Nº 510, DE 07 DE ABRIL DE 2016. Normas Aplicáveis a Pesquisas em Ciências Humanas e Sociais.

http://conselho.saude.gov.br/resolucoes/2016/Reso510.pdf

★ RESOLUÇÃO Nº 580, DE 22 DE MARÇO DE 2018. Especificidades éticas das pesquisas de interesse estratégico para o Sistema Único de Saúde (SUS)

https://conselho.saude.gov.br/resolucoes/2018/Reso580.pdf

Documento publicado em 02/10/2023 (vigência até 31/12/2024)