

1. PREÂMBULO

1.1. **Contexto.** Esta Política foi formulada a partir de uma avaliação preliminar, realizada em reunião de trabalho ocorrida no dia 11 de junho de 2021, na qual foram discutidos os desafios do Instituto de Estudos para Políticas de Saúde (“IEPS”) quanto ao tema da proteção de dados pessoais. Diversas rodadas de troca de informações se seguiram até chegarmos neste ponto conclusivo. Também leva em consideração o diagnóstico técnico realizado pela empresa Pragma Code, representado pelo documento “*Avaliação Técnica de Infraestrutura - Adequação à LGPD*” (Anexo I).

1.2. **Fundamento.** Este documento observa a Lei Geral de Proteção de Dados (LGPD), especialmente em seu art. 50, § 1º, que determina que na criação de políticas de segurança de dados serão observados “a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular”. Diante da norma legal e das condições institucionais e administrativas do IEPS, foi assumida a premissa de que o tratamento de dados pessoais, no âmbito da organização, não tem e nem se aproxima de qualquer finalidade comercial e se volta, prioritariamente, às atividades, projetos e pesquisas que configuram suas finalidades sociais, como definidas pelo seu Estatuto.

1.3. **Objetivos.** São dois os objetivos principais desta política: ser um documento compreensível pelos seus destinatários e destinatárias e, ainda, dinamicamente atualizável, diante dos desafios que a segurança da informação e da proteção de dados pessoais imponham à realidade do IEPS.

2. DEFINIÇÕES

2.1. **Dado pessoal,** nos termos da lei e para os fins desta Política, é a informação sobre pessoa natural identificada ou identificável, que pode ser também qualificado como *sensível*, desde que envolva 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 e dado genético ou biométrico.

2.2. Lei 13.709/18 é a [LGPD](#), que define o regime jurídico aplicável ao tratamento de dados pessoais, estabelece os direitos dos *titulares de dados pessoais (a quem os dados se referem)*, fixando, ainda, condições para a observância desses direitos por pessoas físicas e jurídicas, com ou sem fins lucrativos, e fixando um sistema de responsabilização e de sanções para hipóteses de violação a esses direitos.

2.3. IEPS, para os fins legais e desta Política, será o *controlador* dos dados pessoais quando estiver, por força de lei, na posição de decidir a respeito do tratamento de dados pessoais. Também poderá figurar na posição de *operador*, quando, pelas circunstâncias, realizar o tratamento de dados pessoais em nome de uma outra instituição controladora (por exemplo, em uma parceria com ente público que compartilhe dados pessoais com o IEPS para uma pesquisa).

2.4. **Banco de dados** é o conjunto estruturado de dados pessoais mantido pelo IEPS, justificadamente, para os fins legais, em suporte eletrônico ou físico, e que deverá ser organizado e atualizado continuamente.

2.5. **Incidente de segurança** é caracterizado como qualquer evento que possa acarretar risco ou dano relevante aos titulares cujos dados pessoais estejam no Banco de dados do IEPS, devendo ser comunicado, na forma da lei, à Autoridade Nacional de Proteção de Dados (ANPD).

3. DIRETRIZES

3.1. Providências e normas internas. Na execução desta Política, o IEPS implementará ou observará, dentre outras medidas:

3.1.1. Tratamento de dados pessoais pelo IEPS. O tratamento de dados pessoais por todos(as) colaboradores e pelo corpo diretivo do IEPS atenderá, sempre, a propósitos legítimos, específicos, compatíveis com as finalidades informadas ao seu titular e limitados ao que seja estritamente necessário.

3.1.2. Eliminação e restrição de coleta de dados pessoais. O IEPS eliminará, de forma segura, dados pessoais desnecessários mantidos em seu Banco de dados, assim como evitará a coleta de dados pessoais que não sejam imprescindíveis para suas atividades, restringindo, também, ao máximo possível, o número de colaboradores(as) que tenham acesso a esses dados.

3.1.2.1. Dados pessoais armazenados em meio digital. Os dados que não sejam mais necessários, tais como currículos, cópias de documentos pessoais, imagens de ambiente e quaisquer outras informações disponíveis em meio digital e que permitam a identificação pessoal deverão ser descartados de forma segura. Mídias devem ser trituradas e backups devem ser verificados para eliminar completamente informações desnecessárias.

3.1.2.2. Dados pessoais armazenados em meio físico. Os dados armazenados em meio físico devem ser triturados, para eliminar completamente a informação desnecessária.

3.1.2.3. Acesso a espaços físicos do IEPS. O acesso aos espaços físicos dos escritórios deve ser regulado através de cadastro e/ou biometria, limitando assim a exposição de eventuais dados pessoais dispostos ali.

3.1.3. Observância das condições legais para o tratamento de dados. Nas atividades do IEPS serão estabelecidas medidas que impeçam ou dificultem o tratamento de dados pessoais antes do cumprimento de requisitos necessários, a exemplo de consentimento do titular de dados, da verificação das condições jurídicas aplicáveis, de formalização de contratos ou acordos, entre outras medidas.

3.1.4. Definição de um encarregado de dados pessoais. Será a pessoa indicada para atuar como canal de comunicação entre o IEPS, os titulares dos dados e a ANPD. Até que sobrevenha a norma de que trata o art. 41, § 3º, da LGPD, a identificação e o e-mail de contato do encarregado de dados poderão ser divulgados junto à política de privacidade do site do IEPS. O encarregado de dados pessoais receberá formação específica para o exercício de suas atribuições e deverá ser um agente interno de sensibilização dos(as) colaboradores(as) para esse assunto.

3.1.5. Aplicação da Política às atividades, projetos e pesquisas. Nenhuma atividade, projeto ou pesquisa será iniciado pelo IEPS sem a observância desta Política.

3.1.6. Sensibilização. O IEPS promoverá, sempre que possível, a sensibilização e a capacitação de sua equipe e do corpo diretivo sobre a importância desta Política, pelos meios que entender mais eficazes.

3.1.7. Compartilhamento de dados pessoais. O uso compartilhado de dados entre o IEPS e outras instituições observará as condições legais aplicáveis e será objeto de disciplina contratual específica.

- 3.1.8. Acordo de confidencialidade.** O IEPS adotará um modelo de acordo de confidencialidade que poderá ser ajustado e aplicado às diversas relações em que seja necessário.
- 3.1.9. Seleção de fornecedores e parceiros.** O IEPS selecionará fornecedores, prestadores de serviço e parceiros que demonstrem alinhamento às normas da LGPD e compromisso com políticas consistentes de segurança da informação.
- 3.1.10. Reavaliação de contratos.** O IEPS reavaliará contratos e acordos pré-existentes à esta Política, incluindo parcerias, contratos de prestação de serviços, contratos de trabalho, de estágio, e outros, no que couber, visando promover sua adequação à LGPD.
- 3.1.11. Sistemas de segurança da informação.** O IEPS deverá prover, dentro do possível, sistemas de segurança da informação adequados e compatíveis com sua estrutura, incluindo: antivírus, softwares de monitoramento, gerenciador de senhas e informações confidenciais e quaisquer outras medidas recomendadas por sua consultoria de suporte nessa área para o uso corporativo.
- 3.1.12. Atualizações e restrições de acesso.** Deverá ser garantida, em especial, a atualização e as restrições de acesso ao parque de equipamentos do IEPS, conforme as diretrizes da consultoria especializada.
- 3.1.13. Segurança de redes *wifi*.** Serão disponibilizadas redes *wifi* segregadas para visitantes, assegurando-se o bloqueio da rede física apenas para equipamentos previamente cadastrados.

3.1.14. Senhas. Preferencialmente, as senhas de acesso individuais a e-mails corporativos, sistemas internos e quaisquer outras informações confidenciais deverão ser armazenadas pelos(as) colaboradores(as) em um gerenciador de senhas provido pelo IEPS. As senhas devem ser alteradas periodicamente.

3.1.15. Acesso remoto por dispositivos móveis e outros equipamentos externos. As regras desta Política devem ser observadas, na maior medida possível, pelos(as) colaboradores(as), no uso de dispositivos externos, não pertencentes ao IEPS.

4. APROVAÇÃO, SUPERVISÃO, REVISÃO E VIGÊNCIA DA POLÍTICA

4.1. Critérios para a aplicação desta Política. O IEPS adotará, dentre outras medidas, as seguintes providências visando a melhor execução desta Política:

4.1.1. Aprovação prévia. Todos os documentos que dão suporte à Política de Segurança da Informação e Proteção de Dados Pessoais, inclusive suas atualizações, serão levados ao conhecimento da Diretoria, que deverá submeter a matéria à deliberação do Conselho Deliberativo e determinar, ao final, o seu registro junto à respectiva ata.

4.1.2. Supervisão. A Diretoria do IEPS reportará ao Conselho Deliberativo, sempre que possível, as providências relativas à implementação desta Política, assim como sobre qualquer outra circunstância relevante que decorra de sua aplicação.

4.1.3. Revisão. Esta Política e os demais documentos de amparo à proteção de dados pessoais poderão ser revistos, pelo IEPS, anualmente, ou sempre

que a regulação pelos órgãos competentes exigir alterações textuais, com posterior ratificação pelo órgão de deliberação superior.

4.1.3.1. Regulação. Toda e qualquer norma legal ou regulamentar que produza reflexos na aplicação desta Política será imediatamente observada pelo IEPS, a despeito de sua incorporação expressa aos documentos internos.

4.1.3.2. Boas práticas. A aplicação desta Política não exclui, ainda, a observância de boas práticas e orientações advindas, por exemplo, de normas setoriais de autorregulação, desde que pertinentes à realidade institucional e administrativa do IEPS.

4.1.3.3. Incidentes de segurança. A ocorrência de incidentes de segurança também poderá ensejar a revisão desta Política, conforme exigirem as particularidades do caso.

4.2. Vigência. Esta Política entra em vigor em 23 de novembro de 2021.

São Paulo, 23 de novembro de 2021