Política de Privacidade e Proteção de Dados Pessoais

OBJETIVO

Art. 1º. Esta Política de Privacidade e Proteção de Dados ("Política") tem como objetivo orientar sobre os procedimentos necessários para tratamento de dados pessoais e as melhores práticas a serem adotadas pela Fundação HEMOPE em seu âmbito interno.

ABRANGÊNCIA

Art. 2º. Esta Política se destina a todos os servidores, empregados, prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades de tratamento de dados pessoais, estendendo-se àqueles que realizem tratamento de dados pessoais em nome desta Fundação HEMOPE.

§ 1º Cada um dos indicados no *caput* é responsável pelo tratamento de dados que conduz e pelo controle das informações tratadas em suas atividades diárias, incluindo os equipamentos fornecidos pela Fundação HEMOPE que estão sob sua responsabilidade.

§ 2º As responsabilidades e os papéis pela proteção de dados pessoais estão detalhados na seção ESTRUTURA DE RESPONSABILIDADES E PAPÉIS desta Política de Proteção de Dados Pessoais Local (PPDPL) da Fundação HEMOPE.

Art. 3º. Esta Política abrange todas as informações de pessoas físicas, sejam informações que identifiquem diretamente ou que possam identificá-las de qualquer forma ("Dados Pessoais"), tratadas em qualquer formato (eletrônico ou impresso).

Art. 4º. Este documento foi elaborado, considerando as seguintes legislações:

I) Lei Federal nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD);

II) Lei Federal nº 12.965, de 23 de abril de 2014: Marco Civil da Internet – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

III) Lei Federal nº 12.527, de 18 de novembro de 2011: Lei de Acesso à Informação – Regula o acesso a informações previsto na Constituição Federal;

IV) Lei Estadual nº 14.804, de 29 de outubro de 2012: Lei de Acesso à Informação – Regula o acesso a informações, no âmbito do Poder Executivo Estadual;

V) Decreto Estadual n° 49.265, de 6 de agosto de 2020: Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual, alterado pelo Decreto Estadual nº 51.745, de 28 de outubro de 2021;

VI) Decreto Estadual nº 49.914, de 10 de dezembro de 2020: Institui a Política Estadual de Segurança da Informação – PESI, no âmbito da administração pública estadual; e,

VII) Portaria nº 26 de 14 de outubro de 2021 da ATI (Doc. SEI 17847488), que contém a Política de Proteção de Dados Pessoais Local (PPDPL).

CONCEITOS E DEFINIÇÕES

Art. 5º. Para o perfeito entendimento deste documento, é importante deixar claro os seguintes conceitos e definições:

I) **ANPD** - Autoridade Nacional de Proteção de Dados: órgão da administração pública federal integrante da Presidência da República e, a despeito de ser órgão, os membros de seu Conselho, embora designados pelo Presidente da República, têm mandato e somente o perderão em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar, o que reforça a autonomia técnica da autoridade;

II) **Agente de Tratamento:** o controlador e o operador;

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

IV) **Controles internos de proteção de dados pessoais:** conjunto de políticas, procedimentos, rotinas e medidas técnicas e administrativas adotados pela Fundação HEMOPE para prevenir, detectar e corrigir falhas no tratamento de dados pessoais e para mitigar os riscos identificados;

V) **Consentimento**: autorização livre, informada e inequívoca (sem deixar dúvidas) pela qual o Titular concorda com o tratamento de seus dados pessoais para uma finalidade previamente estipulada. Após conceder o consentimento, o Titular pode revogá-lo a qualquer tempo para tratamentos futuros, sendo mantido, porém, o tratamento realizado até aquele momento;

VI) **Dado pessoal**: informação relacionada à pessoa natural identificada ou identificável;

VII) **Dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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;

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

IX) **Incidente de segurança com dados pessoais:** qualquer evento adverso confirmado relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade ou autenticidade da segurança de dados pessoais;

X) **Inventário de Dados Pessoais:** registro das operações de tratamento de dados pessoais realizadas pela Fundação HEMOPE, contendo, no mínimo, a finalidade, a base legal, as

categorias de dados e de titulares, os compartilhamentos, o prazo de retenção e as medidas de segurança aplicáveis, nos termos do art. 37 da LGPD e do § 4º do art. 18 do Decreto Estadual nº 49.265/2020;

XI) **Operador de dados**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XII) **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, nos termos do inciso XVII do art. 5º da LGPD;

XIII) **Risco à proteção de dados pessoais:** possibilidade de ocorrência de evento que afete negativamente os direitos e as liberdades dos titulares ou comprometa a conformidade do tratamento com a legislação, mensurada em função de sua probabilidade e de seu impacto;

XIV) **Titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XV) **Tratamento**: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

AGENTES DE TRATAMENTO

Art. 6º. A LGPD dispõe sobre o controlador e o operador como os agentes de tratamento de Dados Pessoais, com obrigações previstas na lei, sendo o controlador pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais e o operador, por sua vez, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Parágrafo único: Em observância à PPDPL, os tipos de operadores relacionados à Fundação HEMOPE poderão ser os seguintes:

I) Operador Contratado - Pessoa natural e/ou jurídica de direito privado que exerce atividade de tratamento de dados em nome da Fundação HEMOPE por força de sua relação contratual com esta ou convênio, limitado ao estabelecido objetivamente neste instrumento;

II) Operador Público - Pessoa jurídica de direito público que, através de seu corpo funcional, exerce atividade de tratamento de dados em nome da Fundação HEMOPE por força de sua relação institucional com o Governo de Pernambuco ou através de convênios com outros entes.

Art. 7º Para efeito desta Política, a atuação principal da Fundação HEMOPE será como controladora referentes ao tratamento de dados pessoais sob a sua guarda.

ESTRUTURA DE RESPONSABILIDADES E PAPÉIS

Art. 8º. A estrutura de responsabilidades e papéis pela proteção de dados pessoais na Fundação HEMOPE, estabelecida em observância ao inciso II do § 1º do art. 6º e aos arts. 12 e 13 do Decreto Estadual nº 49.265/2020, é composta por:

I) Controlador;
II) Encarregado pelo tratamento de dados pessoais e sua equipe de apoio;
III) Gestores das unidades organizacionais;
IV) Unidade responsável pela Tecnologia da Informação;
V) Unidade de assessoramento jurídico;
VI) Ouvidoria;
VII) Usuários internos; e
VIII) Operadores.

Parágrafo único. A atuação dos papéis previstos no *caput* observará as competências atribuídas ao Comitê Executivo de Governança Digital, ao Comitê Técnico de Governança Digital, à Secretaria da Controladoria-Geral do Estado, à Agência de Tecnologia da Informação (ATI) e à Procuradoria-Geral do Estado pelos arts. 7º a 11 do Decreto Estadual nº 49.265/2020.

Art. 9º. Compete ao Controlador, representado pelo dirigente máximo da Fundação HEMOPE, nos termos do art. 12 do Decreto Estadual nº 49.265/2020:

I) aprovar, prover condições e promover ações para a efetividade desta Política;
II) designar, por ato próprio, o Encarregado e sua equipe de apoio, observadas as prerrogativas e qualificações necessárias ao exercício da função, assegurando-lhe subordinação direta, assessoria jurídica e tecnológica e poderes para tratar questões que afetem os operadores;
III) elaborar o Relatório de Impacto à Proteção de Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da Fundação HEMOPE;
IV) fornecer aos operadores termos de uso, manuais de instruções e treinamento dos tratamentos sob sua responsabilidade;
V) aprovar os critérios de aceitação de riscos, a Matriz de Riscos e o Plano de Tratamento de Riscos de que trata esta Política, bem como decidir, de forma fundamentada, sobre a aceitação de riscos de nível alto ou crítico; e
VI) estabelecer objetivos e metas próprios de proteção de dados pessoais, de acordo com a maturidade e a capacidade operacional da Fundação HEMOPE, em consonância com o Plano Quadrienal Estratégico de Proteção de Dados Pessoais (PPDP).

Art. 10. Compete ao Encarregado e à sua equipe de apoio, nos termos do art. 13 do Decreto Estadual nº 49.265/2020:

I) gerenciar esta Política para:
   a) inventariar os tratamentos do controlador, inclusive os eletrônicos, mantendo atualizado o Inventário de Dados Pessoais;
   b) analisar a maturidade dos tratamentos em face dos objetivos e metas estabelecidos e do consequente risco de incidentes de privacidade;
   c) avaliar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;
   d) adotar as providências cabíveis para implementar as medidas de segurança avaliadas; e
   e) cumprir os objetivos e metas previstos nesta Política;
II) receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, em articulação com a Ouvidoria;
III) receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;
IV) orientar os servidores, empregados, colaboradores e contratados no cumprimento das práticas necessárias à privacidade de dados pessoais;
V) quando provocado, entregar o Relatório de Impacto à Proteção de Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica;
VI) atender às normas complementares da ANPD;
VII) informar à ANPD e aos titulares dos dados pessoais eventuais incidentes de segurança com dados pessoais, no âmbito da execução do Plano de Resposta a Incidentes; e
VIII) coordenar o processo de gerenciamento de riscos e o monitoramento dos controles internos de proteção de dados pessoais, consolidando a Matriz de Riscos e reportando seus resultados ao Controlador.

Parágrafo único. A equipe de apoio ao Encarregado será designada por ato do dirigente máximo e contará, no mínimo, com representantes das unidades de tecnologia da informação, de assessoramento jurídico e de ouvidoria.

Art. 11. Compete aos gestores das unidades organizacionais, na qualidade de responsáveis pelos processos de tratamento de dados pessoais sob sua gestão:

I) informar ao Encarregado os tratamentos de dados pessoais realizados em sua unidade e manter atualizadas as respectivas informações no Inventário de Dados Pessoais;
II) identificar, analisar e tratar os riscos à proteção de dados pessoais dos processos sob sua gestão, com o apoio do Encarregado;
III) implementar e executar os controles internos e as ações mitigadoras aplicáveis à sua unidade;

IV) comunicar previamente ao Encarregado a criação de novos tratamentos, a alteração de finalidade, a implantação de sistemas ou a contratação de serviços que envolvam dados pessoais, para avaliação da necessidade de elaboração ou atualização do Relatório de Impacto à Proteção de Dados Pessoais;

V) fornecer as informações necessárias à elaboração do Relatório de Impacto à Proteção de Dados Pessoais; e

VI) comunicar imediatamente ao Encarregado qualquer incidente de segurança com dados pessoais de que tenha conhecimento.

Art. 12. Compete à unidade responsável pela Tecnologia da Informação:

I) implementar e manter as medidas técnicas de segurança aplicáveis aos dados pessoais, em alinhamento com a Política Estadual de Segurança da Informação e com as orientações da Agência de Tecnologia da Informação (ATI);

II) prestar apoio técnico à elaboração do Relatório de Impacto à Proteção de Dados Pessoais e à análise de riscos dos sistemas de informação;

III) observar a proteção de dados pessoais desde a concepção e por padrão no desenvolvimento, na aquisição e na manutenção de soluções de tecnologia da informação; e

IV) atuar na detecção, contenção e registro de incidentes de segurança com dados pessoais, no âmbito do Plano de Resposta a Incidentes.

Art. 13. Compete à unidade de assessoramento jurídico:

I) prestar apoio jurídico à elaboração do Relatório de Impacto à Proteção de Dados Pessoais;

II) orientar quanto à identificação das bases legais aplicáveis aos tratamentos de dados pessoais; e

III) zelar pela inclusão de cláusulas de proteção de dados pessoais em contratos, convênios e instrumentos congêneres, observados os modelos disponibilizados pela Procuradoria-Geral do Estado.

Art. 14. Compete à Ouvidoria receber as solicitações dos titulares de dados pessoais, inclusive por meio dos canais da Ouvidoria-Geral do Estado, encaminhá-las ao Encarregado e acompanhar a sua resolutividade, nos termos dos arts. 14 a 16 do Decreto Estadual nº 49.265/2020.

Art. 15. Compete aos usuários internos, compreendidos como os servidores, empregados, estagiários, colaboradores e demais pessoas indicadas no art. 2º desta Política:

I) cumprir esta Política e as normas e procedimentos dela decorrentes;

II) tratar somente os dados pessoais necessários ao desempenho de suas atribuições;

III) participar das ações de capacitação e conscientização em proteção de dados pessoais; e

IV) comunicar imediatamente ao Encarregado ou ao gestor de sua unidade qualquer incidente de segurança com dados pessoais de que tenha conhecimento.

Art. 16. Compete aos operadores, contratados ou públicos:

I) realizar o tratamento de dados pessoais segundo as instruções fornecidas pela Fundação HEMOPE e exclusivamente para as finalidades pactuadas;
II) adotar medidas de segurança técnicas e administrativas compatíveis com as exigidas nesta Política;
III) comunicar à Fundação HEMOPE, sem demora, qualquer incidente de segurança com dados pessoais;
IV) colaborar com a elaboração do Relatório de Impacto à Proteção de Dados Pessoais e com as verificações de conformidade, quando solicitado; e
V) devolver ou eliminar os dados pessoais ao término da relação contratual ou do convênio, ressalvadas as hipóteses legais de conservação.

TRATAMENTO DE DADOS PESSOAIS

Art. 17. As atividades de tratamento de dados pessoais realizadas pela Fundação HEMOPE devem respeitar os princípios previstos da LDPD, tais como: boa-fé; finalidade legítima, específica e explícita; adequação; livre acesso; qualidade; transparência; segurança e prevenção; e não discriminação.

Art. 18. A Fundação HEMOPE, por meio de suas diversas áreas, processos e sistemas, pode coletar e tratar dados pessoais para finalidades específicas e com a devida transparência ao titular.

Art. 19. A Fundação HEMOPE poderá realizar o tratamento de dados pessoais de acordo com o expresso e inequívoco consentimento do usuário ou, ainda, de acordo com as bases legais previstas no Art. 7º e no Art. 11 da LGPD, tais como:

I) para o cumprimento de obrigação legal ou regulatória;
II) pela administração pública, para a execução de políticas públicas, incluindo o tratamento e uso compartilhado de dados;
III) para a realização de estudos por órgão de pesquisa, via anonimização dos dados pessoais, sempre que possível;
IV) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular;
V) para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
VI) para a proteção da vida ou da segurança física do titular ou de terceiro;
VII) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
VIII) quando necessário para atender ao legítimo interesse do controlador ou de terceiro;

IX) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente; e

X) atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências ou cumprir as atribuições legais do serviço judicial.

Art. 20. A Fundação HEMOPE também pode tratar dados pessoais com base em legítimos interesses, desde que prevaleçam os direitos e liberdades fundamentais dos titulares.

§1º Nas hipóteses do *caput*, os dados pessoais são tratados com base em legítimos interesses para garantir a prestação de serviços que lhes beneficiem, executar análises internas, bem como para o apoio, realização e promoção das nossas atividades.

§2º A finalidade do tratamento deve ser indicada e pautada em fundamentações claras e legítimas, a partir de situações concretas, somente se coletando os dados estritamente necessários para esse objetivo.

COMPARTILHAMENTO DE DADOS PESSOAIS

Art. 21. Para a execução das atividades da Fundação HEMOPE, sempre que necessário, esta Fundação poderá compartilhar os dados pessoais com outras instituições, desde que com previsão legal de atribuição, com prestadores de serviço ou parceiros, dentro dos limites legais e contratuais, sendo o rol abaixo meramente exemplificativo:

I) **Prestadores de serviço que são operadores de dados pessoais da Fundação HEMOPE:** para que possamos disponibilizar nossos serviços com qualidade, contamos com a colaboração de alguns prestadores de serviço, que tratam os dados pessoais coletados em nosso nome e de acordo com nossas instruções e finalidades específicas. O acesso de terceiros às informações coletadas pela Prestadora de Serviço se dá exclusivamente para atendimento das finalidades informadas em contrato e dentro do limite necessário ao desempenho das atividades da instituição.

II) **Controladores conjuntos (Co-controladores):** A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um controlador, os quais serão responsáveis por determinar conjuntamente as finalidades e os meios de tratamento dos dados. Estes, por meio de acordo, irão estabelecer as respectivas responsabilidades quanto ao cumprimento da LGPD.

III) **Autoridades governamentais:** nós devemos fornecer dados pessoais em atendimento à ordem judicial, solicitações de autoridades administrativas com prerrogativas legais de acesso, obrigação legal ou regulatória, bem como para agir de forma colaborativa com autoridades governamentais. Cumpre destacar que todos os dados pessoais serão compartilhados com autoridades administrativas dentro dos limites da Lei.

Art. 22. A Fundação HEMOPE manterá contratos com terceiros para o fornecimento de produtos ou a prestação de serviços necessários a suas operações, os quais poderão, conforme o caso, importar em disciplina própria de proteção de dados pessoais, a qual deverá estar disponível e ser consultada pelos interessados.

§1º Os Parceiros da Fundação HEMOPE são autorizados a utilizar seus Dados Pessoais somente para os fins específicos para os quais eles foram contratados.

§2º A Fundação HEMOPE firma compromisso contratual com seus parceiros a fim de que sejam tomadas medidas de segurança adequadas à proteção de seus Dados Pessoais.

Art. 23. Na hipótese de compartilhamento de dados com terceiros fora do setor público, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados, garantindo-lhes o exercício aos direitos previstos no art. 18 da LGPD, com destaque aos direitos de acesso, retificação, oposição, eliminação e informação das entidades públicas e privadas com as quais o controlador irá realizar o uso compartilhado de dados.

§ 1º A comunicação ao titular será renovada na alteração da finalidade ou em qualquer alteração nas operações de tratamento, inclusive de novo compartilhamento ou transferência.

§ 2º A cada tratamento de dados será feita uma análise acerca do cumprimento dos princípios da necessidade e adequação pelo controlador.

§ 3º Nos casos de tratamento de dados feitos com base no consentimento, cada nova operação realizada com os dados pessoais deve ser objeto de nova requisição de consentimento, inclusive para o compartilhamento dos dados com outras entidades, dentro ou fora da administração pública.

Art. 24. A transparência dos compartilhamentos será proporcionada nos termos da Lei de Acesso à Informação Estadual – Lei nº 14.804, de 29 de outubro de 2012 e do Decreto nº 49.265, de 6 de agosto de 2020.

DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

Art. 25. O Tratamento de Dados Pessoais de crianças e adolescentes sempre deverá ser realizado com o Consentimento específico e em destaque de um dos seus pais ou responsável legal, atendendo aos critérios exigidos na legislação.

Parágrafo Único: O uso dos Dados Pessoais de crianças e adolescentes deverá observar seu melhor interesse, sendo proibido a utilização ou condicionamento para a participação em jogos, aplicações de internet ou outras atividades além do estritamente necessário para a atividade.

Art. 26. As informações sobre o Tratamento de Dados de crianças e adolescentes serão fornecidas sempre de maneira simples, clara e acessível e a Fundação HEMOPE deverá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o

exercício dos direitos previstos pela LGPD.

Art. 27. A coleta de dados de crianças poderá ser realizada sem o consentimento apenas quando necessário para o contato dos pais ou responsável legal, podendo ser utilizado uma única vez e sem armazenamento, ou para sua proteção, sem possibilidade de compartilhamento desta informação com prestadores de serviços.

DADOS PESSOAIS SENSÍVEIS

Art. 28. O tratamento de dados pessoais sensíveis é restrito e somente realizado em uma ou mais das seguintes hipóteses legais:

I) Cumprimento de obrigações legais e/ou regulatórias;

II) Execução de políticas públicas previstas em leis ou regulamentos;

III) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

IV) Proteção da sua vida ou da sua incolumidade física ou da vida e da incolumidade física de terceiros;

V) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

VI) Garantia da prevenção à fraude e à sua segurança, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados na legislação aplicável e nesta Política e exceto no caso de prevalecerem seus direitos e liberdades fundamentais que exijam a proteção dos dados pessoais.

Art. 29. A Fundação HEMOPE também pode tratar dados pessoais sensíveis quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas, tendo este titular o direito de revogar o seu consentimento a qualquer tempo, o que não afeta:

I) a legalidade do tratamento de dados pessoais sensíveis baseado no seu consentimento antes da revogação; e/ou

II) a legalidade do tratamento de dados pessoais sensíveis baseado em outras hipóteses legais.

DIREITOS DO TITULAR DOS DADOS PESSOAIS

Art. 30. A transparência sobre o tratamento dos seus dados pessoais é prioridade para a Fundação HEMOPE, motivo pelo qual, além das informações disponibilizadas nesta Política, o titular de dados

poderá exercer os direitos previstos na Lei Geral de Proteção de Dados, tais como:

I) Confirmação da existência de tratamento de dados pessoais;
II) Acesso aos dados pessoais;
III) Revogação do consentimento, caso seja possível a eliminação do dado;
IV) Correção de dados pessoais incompletos, inexatos ou desatualizados;
V) Oposição ou restrição ao tratamento dos dados pessoais quando realizado em desacordo com os requisitos da LGPD;
VI) Eliminação dos dados pessoais tratados com o consentimento ou desnecessários, excessivos ou quando entender que algum ponto da LGPD não foi atendido;
VII) Informação sobre as hipóteses e com quais parceiros e outras instituições podemos compartilhar, ou receber dados pessoais referentes a você;
VIII) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, quando aplicável; e,
IX) Apresentação de reclamação perante a Autoridade Nacional de Proteção de Dados.

Art. 31. Todas as solicitações serão apresentadas de forma gratuita, e submetidas a uma prévia avaliação da sua identidade e da viabilidade do atendimento enviando um e-mail para o Encarregado pelo tratamento de dados pessoais, a fim de cumprir com eventuais obrigações que impeçam o completo atendimento das requisições dos titulares de direito.

SEGURANÇA E INCIDENTES COM DADOS PESSOAIS

Art. 32. A Fundação HEMOPE, de acordo com a sua Política de Segurança da Informação, deve adotar medidas de segurança da informação, técnicas e administrativas visando à proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Parágrafo Único: A Fundação HEMOPE reportará os incidentes de segurança com dados pessoais eventualmente detectados por meio do Plano de Resposta a Incidentes previsto na seção CONTROLES INTERNOS DE PROTEÇÃO DE DADOS PESSOAIS desta Política, em conformidade com sua Política interna de Segurança da Informação e com a Política Estadual de Segurança da Informação.

Art. 33. No tratamento das informações coletadas, a Fundação HEMOPE utiliza sistemas estruturados de forma a atender os requisitos de segurança e transparência, aos padrões de boas práticas e de governança e aos princípios gerais estabelecidos na Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 34. O acesso às informações coletadas é restrito aos colaboradores e pessoas autorizadas, estando sujeitos às sanções administrativas, disciplinares e legais cabíveis aqueles que se utilizarem indevidamente destes dados.

Art. 35. Todos aqueles que realizarem o tratamento de dados pessoais deverão se comprometer a manter o sigilo absoluto das informações acessadas, bem como adotar as melhores práticas para manuseio destas informações, conforme determinado nas políticas e normas internas.

Art. 36. Ao identificar qualquer situação que possa ocasionar uma violação de dados pessoais, deve-se encaminhar um e-mail para o Encarregado, para adoção das providências cabíveis, no endereço indicado nesta Política.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Art. 37. A Fundação HEMOPE, na qualidade de controladora, elaborará o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), na forma dos arts. 5º, inciso XVII, e 38 da LGPD, e nos termos do inciso III do art. 12 e do inciso V do art. 13 do Decreto Estadual nº 49.265/2020, com o apoio técnico das áreas jurídica e tecnológica.

§ 1º Compete ao Controlador a elaboração e a aprovação do RIPD, e ao Encarregado a coordenação de sua elaboração, a sua guarda e a sua entrega, quando provocado, à ANPD, aos órgãos de controle ou a outras autoridades competentes.

§ 2º Na elaboração do RIPD serão utilizados, preferencialmente, os modelos e manuais disponibilizados pela Secretaria da Controladoria-Geral do Estado e as orientações da ANPD.

Art. 38. O RIPD deverá ser elaborado ou atualizado nas seguintes hipóteses:

I) previamente ao início de tratamento de dados pessoais que possa gerar alto risco às liberdades civis e aos direitos fundamentais dos titulares, observados os critérios definidos pela ANPD, considerando-se como tal, em especial, o tratamento em larga escala de dados pessoais sensíveis referentes à saúde, de dados genéticos ou biométricos e de dados de crianças e adolescentes, inerente às atividades hematológicas e hemoterápicas da Fundação HEMOPE;
II) na implantação de novos sistemas de informação ou na alteração relevante de sistemas, processos ou contratações que envolvam tratamento de dados pessoais de alto risco;
III) quando o tratamento tiver como fundamento o legítimo interesse do controlador;
IV) quando houver alteração relevante na natureza, no escopo, no contexto ou na finalidade do tratamento, ou após a ocorrência de incidente de segurança relevante; e
V) mediante solicitação da ANPD ou de órgão de controle.

Art. 39. O RIPD conterá, no mínimo:

I) a identificação do controlador, do Encarregado e dos operadores envolvidos;
II) a descrição da natureza, do escopo, do contexto e da finalidade do tratamento;
III) os tipos de dados pessoais coletados, com destaque para os dados pessoais sensíveis e os de crianças e adolescentes;
IV) a base legal que fundamenta o tratamento;
V) a metodologia utilizada para a coleta e para a garantia da segurança das informações;
VI) a avaliação da necessidade e da proporcionalidade do tratamento;
VII) a identificação e a avaliação dos riscos, conforme o processo de gerenciamento de riscos estabelecido nesta Política;
VIII) a análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados; e
IX) a manifestação do Encarregado e a aprovação do Controlador.

Art. 40. O RIPD será revisado, no mínimo, anualmente, em consonância com o ciclo anual de monitoramento da Política Estadual de Proteção de Dados Pessoais, e sempre que ocorrer qualquer das hipóteses previstas no art. 38 desta Política.

PROCESSO DE GERENCIAMENTO DE RISCOS

Art. 41. O gerenciamento de riscos à proteção de dados pessoais da Fundação HEMOPE, estabelecido em observância ao inciso III do § 1º do art. 6º do Decreto Estadual nº 49.265/2020, considerará a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento, em alinhamento com a Política Estadual de Segurança da Informação, e compreenderá as seguintes etapas:

I) estabelecimento do contexto: identificação dos processos, sistemas, ativos, titulares e dados pessoais envolvidos, a partir do Inventário de Dados Pessoais;
II) identificação dos riscos: levantamento dos eventos que possam comprometer a confidencialidade, a integridade ou a disponibilidade dos dados pessoais ou os direitos dos titulares, tais como acesso não autorizado, compartilhamento indevido, coleta excessiva, retenção além do prazo necessário e falhas de sistemas;
III) análise dos riscos: estimativa da probabilidade de ocorrência e do impacto de cada risco, considerando os controles existentes;
IV) avaliação dos riscos: comparação do nível de risco com os critérios de aceitação aprovados pelo Controlador, para definição de prioridades;
V) tratamento dos riscos: definição da resposta a cada risco — mitigar, transferir ou compartilhar, evitar ou aceitar — e das ações mitigadoras correspondentes;
VI) monitoramento e análise crítica: acompanhamento da execução das ações mitigadoras e da

eficácia dos controles; e

VII) comunicação e consulta: envolvimento dos gestores, do Encarregado e das áreas técnicas ao longo de todo o processo.

Art. 42. Para a análise de que trata o inciso III do art. 41 desta Política, a probabilidade e o impacto serão classificados em escala de 1 (muito baixo) a 5 (muito alto), e o nível de risco corresponderá ao produto entre ambos, classificado como:

I) baixo: de 1 a 4;
II) médio: de 5 a 9;
III) alto: de 10 a 16;
IV) muito alto: 17 a 19; e
V) crítico: de 20 a 25.

Parágrafo único. Na avaliação do impacto será considerada, com peso preponderante, a natureza sensível dos dados pessoais referentes à saúde, genéticos e biométricos tratados pela Fundação HEMOPE.

Art. 43. Os riscos identificados serão registrados na Matriz de Riscos à Proteção de Dados Pessoais, mantida pelo Encarregado, que conterá, para cada risco, a descrição, o tratamento de dados associado, as causas, as consequências, a probabilidade, o impacto, o nível de risco, os controles existentes, a resposta adotada, as ações mitigadoras, o responsável e o prazo.

§ 1º Os riscos de nível baixo poderão ser aceitos pelo gestor da unidade responsável, mediante registro na Matriz de Riscos.

§ 2º Os riscos de nível médio deverão ser objeto de ações mitigadoras incluídas no Plano de Tratamento de Riscos.

§ 3º Os riscos de nível alto ou crítico somente poderão ser aceitos mediante decisão fundamentada do Controlador e ensejarão a elaboração ou a atualização do RIPD do tratamento correspondente.

Art. 44. O ciclo completo de gerenciamento de riscos será realizado, no mínimo, anualmente, e será reavaliado extraordinariamente quando da criação de novo tratamento, da implantação ou alteração relevante de sistema, de mudança na legislação aplicável, da ocorrência de incidente de segurança com dados pessoais ou de recomendação de auditoria ou de órgão de controle.

Parágrafo único. Os resultados do ciclo anual serão consolidados em relatório elaborado pelo Encarregado, submetido ao Controlador e disponibilizado à Secretaria da Controladoria-Geral do Estado para fins de monitoramento da Política Estadual de Proteção de Dados Pessoais e de acompanhamento dos indicadores do Plano Quadrienal Estratégico de Proteção de Dados Pessoais.

CONTROLES INTERNOS DE PROTEÇÃO DE DADOS PESSOAIS

Art. 45. Em observância aos incisos IV e V do § 1º do art. 6º do Decreto Estadual nº 49.265/2020, a Fundação HEMOPE manterá os seguintes controles internos de proteção de dados pessoais, sem prejuízo de outros definidos a partir do processo de gerenciamento de riscos:

I) controles de governança e conformidade:
   a) Inventário de Dados Pessoais, atualizado pelos gestores das unidades e consolidado pelo Encarregado;
   b) registro dos compartilhamentos de dados pessoais, nos termos do § 1º do art. 19 do Decreto Estadual nº 49.265/2020;
   c) verificação prévia da finalidade, da necessidade e da base legal de cada novo tratamento;
   d) inclusão de cláusulas de proteção de dados pessoais em contratos, convênios e instrumentos congêneres;
   e) divulgação, no sítio eletrônico institucional, de informações claras e atualizadas sobre os tratamentos de dados pessoais realizados; e
   f) programa periódico de capacitação e conscientização em proteção de dados pessoais;

II) controles técnicos e administrativos de segurança:
   a) controle de acesso por perfil, com base no princípio do menor privilégio, revisão periódica das permissões e revogação tempestiva nos casos de desligamento ou mudança de função;
   b) autenticação individual e registro das operações realizadas com dados pessoais, nos termos do § 4º do art. 18 do Decreto Estadual nº 49.265/2020;
   c) utilização de criptografia, pseudonimização ou anonimização sempre que possível;
   d) cópias de segurança periódicas, com testes de restauração;
   e) gestão de vulnerabilidades e atualização dos sistemas e equipamentos;
   f) proteção de documentos físicos que contenham dados pessoais, com guarda em local de acesso controlado;
   g) descarte seguro de documentos e mídias, observada a tabela de temporalidade aplicável; e
   h) assinatura de termo de responsabilidade e confidencialidade pelos usuários internos e operadores;

III) controles de resposta e atendimento:
   a) Plano de Resposta a Incidentes com dados pessoais, contemplando as etapas de detecção, contenção, avaliação, registro e comunicação à ANPD e aos titulares, nos prazos e na forma estabelecidos pela ANPD;
   b) registro de todos os incidentes de segurança com dados pessoais, ainda que não comunicados à ANPD; e
   c) fluxo de atendimento às solicitações dos titulares, com registro e controle de prazos, em articulação com a Ouvidoria; e

IV) controles de monitoramento:

a) indicadores de desempenho alinhados ao Plano Quadrienal Estratégico de Proteção de Dados Pessoais;
b) avaliação anual do nível de maturidade dos tratamentos de dados pessoais; e
c) verificações periódicas de conformidade, observada a sistemática de auditoria interna estabelecida pela Secretaria da Controladoria-Geral do Estado.

Art. 46. As ações mitigadoras dos riscos identificados serão registradas no Plano de Tratamento de Riscos, com indicação do responsável, do prazo e do indicador de acompanhamento, e terão sua execução monitorada pelo Encarregado.

Art. 47. Os gestores das unidades organizacionais são responsáveis pela execução dos controles internos em suas respectivas áreas, cabendo ao Encarregado verificar a sua eficácia e comunicar ao Controlador as não conformidades identificadas, com proposta de medidas corretivas.

RETENÇÃO E DESCARTE DOS DADOS PESSOAIS

Art. 48. A Fundação HEMOPE realizará a retenção dos dados pessoais dos titulares pelo tempo necessário para o cumprimento das finalidades para os quais eles foram coletados, inclusive para fins de cumprimento de obrigações legais, contratuais, prestação de contas ou eventual requisição de autoridades competentes.

Art. 49. O término do tratamento de dados pessoais pela Fundação HEMOPE deverá ocorrer quando:

I) Atingida a finalidade ou o período de tratamento dos dados;
II) Os Dados deixarem de ser necessários ou pertinentes para as operações da Fundação HEMOPE;
III) Houver a solicitação pelo Titular ou a revogação do seu consentimento. Nestes casos, a Fundação HEMOPE deverá garantir que os dados sejam adequadamente descartados ou destruídos, independentemente se estão armazenados em bases de dados, documentos, equipamentos, sistemas, ou mesmo locais físicos; e,
IV) Houver a determinação pela autoridade nacional, na situação de violação à proteção de dados pessoais.

Art. 50. A Fundação HEMOPE, periodicamente, revisará os dados pessoais sob sua tutela, sejam eles mantidos eletronicamente ou em papel, a fim de decidir eliminar quaisquer dados cuja retenção não esteja mais amparada pela lei.

DISPOSIÇÕES TRANSITÓRIAS

Art. 51. Para a implementação dos instrumentos previstos nesta Política, o Encarregado submeterá ao

Controlador, no prazo de até 90 (noventa) dias contados de sua publicação:

I) a versão consolidada do Inventário de Dados Pessoais;

II) a primeira Matriz de Riscos à Proteção de Dados Pessoais, acompanhada do respectivo Plano de Tratamento de Riscos;

III) a relação dos tratamentos que demandam a elaboração de RIPD, com cronograma priorizado segundo o nível de risco; e

IV) o Plano de Resposta a Incidentes com dados pessoais.

Parágrafo único. Os processos, controles internos, responsabilidades e papéis estabelecidos nesta Política têm aplicação imediata a partir de sua publicação, independentemente da conclusão dos instrumentos referidos no *caput*.

ALTERAÇÕES DESTA POLÍTICA DE PRIVACIDADE

Art. 52. A Política de Privacidade poderá ser alterada em virtude de modificações nas práticas de tratamento de dados pessoais e eventual inclusão de novas funcionalidades e serviços.

CONTATO

Art. 53. Para o esclarecimento de dúvidas ou para o exercício dos direitos dos titulares de dados pessoais previstos nesta Política, deve-se entrar em contato com o Encarregado, por meio do seguinte e-mail: encarregado.ppdpl@hemope.pe.gov.br.