POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DA EBSERH

EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

2021

Identificação geral

CNPJ	15.126.437/0001-43
Administração Central	Brasília-DF
Tipo de estatal	Empresa Pública
Acionista controlador	União
Tipo societário	Sociedade por Cotas de Responsabilidade Limitada – Empr Pública
Tipo de capital	Fechado
Abrangência de atuação	Nacional
Setores de atuação	Educação e Saúde
Presidente	**Oswaldo de Jesus Ferreira** Telefone: (61) 3255-8921 E-mail: oswaldo.ferreira@ebserh.gov.br
Auditor Interno	**Adriano Augusto de Souza** Telefone: (61) 3255-8970 E-mail: souza.adriano@ebserh.gov.br
Auditores independentes atuais da Empresa	Audilink & Cia. Auditores
Membros da Diretoria Executiva subscritores da Política de Proteção de Dados Pessoais da Ebserh	**Oswaldo de Jesus Ferreira** Cargo: Presidente CPF: ***.430.927-** **Eduardo Chaves Vieira** Cargo: Vice-Presidente CPF: ***.431.577-** **Giuseppe Cesare Gatto** Cargo: Diretor de Ensino, Pesquisa e Atenção à Saúde CPF: ***.214.558-** **Simone Henriqueta Cossetin Scholze** Cargo: Diretora de Tecnologia da Informação CPF: ***.824.541-** **Iara Ferreira Pinheiro** Cargo: Diretora de Orçamento e Finanças CPF: ***.894.661-** **Erlon Cesar Dengo** Cargo: Diretor de Administração e Infraestrutura CPF: ***.884.910-** **Rodrigo Augusto Barbosa** Cargo: Diretor de Gestão de Pessoas CPF: ***.368.831-**
Data da Divulgação	30/07/2021
Versão	1.0

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DA EBSERH

Dispõe sobre definições, diretrizes e deveres dos integrantes da Rede Ebserh para a proteção de dados pessoais no âmbito da Empresa Brasileira de Serviços Hospitalares (Ebserh).

CAPÍTULO I – ESCOPO DE APLICAÇÃO

Art. 1º Todos que integrem a Rede Ebserh ou que realizem tratamento de dados pessoais em seu nome devem observar as diretrizes indicadas nesta Política, que visam à conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

CAPÍTULO II – DEFINIÇÕES

Art. 2º Para os fins desta Política, considera-se:

I - agentes de tratamento: o controlador e o operador;

II - 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;

III - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Política em todo o território nacional;

IV - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

V - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

VIII - dado pessoal sensível: informação 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;

IX - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

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

XI - operador: 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: 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;

XIII - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento tais como:

a. pacientes, seus responsáveis legais e acompanhantes;
b. estudantes, estagiários, residentes, professores e pesquisadores;
c. empregados, servidores que se encontrem desempenhando suas atividades na Rede

Ebserh e ocupantes de cargos de confiança, e seus dependentes;

d. profissionais de empresas terceirizadas, colaboradores em geral e todos aqueles que, de forma individual ou coletiva, por força de lei, contrato ou qualquer outro ato jurídico, atuam na prestação de serviços à Rede Ebserh, de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, direta ou indiretamente; e

e. outras pessoas que tiverem seus dados pessoais sob os cuidados, ainda que temporariamente, da Rede Ebserh, seja da Administração Central ou dos Hospitais Universitários Federais (HUFs).

XIV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XV - 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; e

XVI - 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.

CAPÍTULO III – PRINCÍPIOS

Art. 3º A proteção de dados pessoais é valor primordial e o tratamento de dados pessoais deve ser cautelosamente avaliado e realizado com observância das diretrizes dispostas nesta Política e na legislação aplicável.

Art. 4º Todo tratamento de dados pessoais realizado no âmbito da Rede Ebserh deve contar com finalidade legítima e específica e estar amparado em uma das disposições previstas na Lei Geral de Proteção de Dados Pessoais.

Art. 5º O tratamento de dados pessoais realizado no âmbito da Rede Ebserh deve observar a boa-fé e os seguintes princípios:

I - finalidade: deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: deve ser garantido ao titular dos dados pessoais a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: devem ser garantidas ao titular dos dados pessoais a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: devem ser garantidas ao titular dos dados pessoais informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos inerentes à atividade;

VII - segurança: devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO IV – DIRETRIZES

Art. 6º A Administração Central e as filiais devem proteger, mapear e registrar o tratamento de dados pessoais realizados no âmbito de suas atuações.

Art. 7ª Os contratos que envolvam tratamento de dados pessoais em nome do controlador devem conter cláusulas que estabeleçam instruções, deveres e obrigações referentes ao tema e o compromisso dos contratados em adotar medidas para adequação de suas operações e cumprimento das legislações de proteção de dados pessoais aplicáveis, bem como desta Política e demais normas e orientações da Ebserh.

Art. 8º Todos os integrantes da Rede Ebserh devem implementar meios para conferir a transparência necessáriaaos titulares em relação ao uso de seus dados pessoais, à finalidade, forma e duração do tratamento, identificação e informações de contato do controlador e do encarregado, informações acerca do uso compartilhado de dados, responsabilidades dos agentesenvolvidos e direitos dos titulares de dados pessoais.

Art. 9º A Administração Central e as filiais devem implementar mecanismos efetivos para atendimento dos direitos dos titulares previstos em lei, como informação, acesso, retificação, portabilidade, eliminação, bloqueio, revogação de consentimento.

Art. 10. Quando a base legal do tratamento for o consentimento, a Rede Ebserh deve implementar mecanismos adequados para a efetiva coleta da autorização dada pelo titular dos dados pessoais e, assim, evidenciar a regularidade do tratamento.

Art. 11. O relatório de impacto à proteção de dados pessoais deve ser elaborado sempre que o tratamento de dados pessoais for capaz de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais ou quando solicitado pela Autoridade Nacional de Proteção de Dados.

Art. 12. A Administração Central e as filiais devem divulgar e manter atualizadas, em seu sítio eletrônico, a identidade e as informações de contato do encarregado pelo tratamento de dados pessoais.

Art. 13. A Administração Central e as filiais devem criar planos de resposta a incidentes que envolvam dados pessoais observado o disposto no Plano de Gestão de Incidentes Cibernéticos da Ebserh.

Art. 14. A Administração Central e as filiais devem atender à obrigação de comunicar a autoridade nacional e aos titulares dos dados pessoais ante a ocorrência de incidentes de segurança.

§ 1º Devem ser estabelecidos prazos de comunicação e resposta, com o fornecimento de subsídios pelas filiais envolvidas, bem como pela Administração Central.

§ 2º O encarregado deverá comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 3º As filiais, quando da necessidade de comunicação com a Autoridade Nacional de Proteção de Dados, deverão fazê-la em alinhamento com a Administração Central.

Art. 15. A Administração Central deve ser sempre comunicada nos casos de incidentes de segurança que envolvam dados pessoais, sejam eles sensíveis ou não.

Art. 16. Toda operação que envolva transferência internacional de dados pessoais deve possuir

salvaguardas, considerando o nível de proteção de dados do país estrangeiro ou organismo internacional do qual o país seja membro, previstas na Lei Geral de Proteção de Dados Pessoais.

Art. 17. A Rede Ebserh deve promover a conscientização dos colaboradores acerca das diretrizes e procedimentos de proteção de dados pessoais implementados.

CAPÍTULO V – CONSENTIMENTO

Art. 18. Dispensa o consentimento o tratamento de dados pessoais realizado com fundamento nas hipóteses previstas na Lei Geral de Proteção de Dados Pessoais.

Art. 19. Caso o consentimento, sendo indispensável, não seja concedido, o tratamento de dados pessoais não será realizado.

Art. 20. O tratamento de dados pessoais de crianças e/ou adolescentes deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

CAPÍTULO VI – DEVERES DOS INTEGRANTES DA REDE EBSERH

Art. 21. No tratamento de dados pessoais, os integrantes da Rede Ebserh devem observar, dentre outros, os seguintes deveres:

I - não disponibilizar nem garantir acesso aos dados pessoais mantidos pela Ebserh para pessoas não autorizadas ou competentes de acordo com as normas da Empresa;

II - obter o consentimento, quando necessário, para o tratamento de dados pessoais;

III - cumprir as normas, recomendações, orientações de segurança da informação e prevenção de incidentes de segurança da informação publicadas pela Ebserh; e

IV - comunicar ao encarregado do tratamento de dados pessoais qualquer evento que possa colocar em risco os dados pessoais tratados pela Rede Ebserh.

Art. 22. Os integrantes da Rede Ebserh que não observarem as diretrizes dispostas nesta Política estãosujeitos às regras de responsabilização previstas em normativos internos e legislação aplicável.

CAPÍTULO VII – DISPOSIÇÕES GERAIS

Art. 23. A Ebserh tratará os dados pessoais em seus próprios sistemas e programas, inclusive por intermédio de terceiros legalmente constituídos, para tanto:

I - utiliza métodos para criptografar e anonimizar os dados coletados;

II - possui proteção contra acesso não autorizado a seus sistemas;

III - autoriza o acesso de pessoas previamente estabelecidas ao local onde são armazenadas as informações coletadas;

IV - cobra de terceiros a manutenção de sigilo, sendo que a quebra acarretará responsabilidade civil e responsabilização conforme a legislação; e

V - envida esforços para preservar a privacidade dos dados dos usuários e estimula estes à autoproteção de seus dados pessoais.

Art. 24. A Administração Central deve editar normativos e recomendações gerais para o tratamento de dados pessoais.

Art. 25. A Administração Central e as filiais devem dar ciência desta Política de Proteção de Dados Pessoais aos fornecedores, prestadores de serviços e partes interessadas.

Art. 26. Ao tomar conhecimento de incidentes de segurança que envolvam dados pessoais, caberá à Administração Central, juntamente com a filial respectiva, analisar a ocorrência e pontuar a gravidade e se houve atendimento das diretrizes desta Política, em especialno que diz respeito aos planos de resposta a incidentes que envolvam dados pessoais.

Art. 27. Esta Política entra em vigor na data de sua publicação.