REGULAMENTO DE GOVERNANÇA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DAS EMPRESAS ELETROBRAS

Edição 1.0
10/08/2020

Regulamento de Governança de Privacidade e Proteção de Dados Pessoais das Empresas Eletrobras

Vinculado à Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras

Área responsável pela emissão

Diretoria de Governança, Riscos e Conformidade / Superintendência de Gestão de Riscos, Controles Internos e Segurança da Informação.

Público-alvo

Empregados, dirigentes, conselheiros e prestadores de serviço das empresas Eletrobras.

Aprovação

Resolução de Diretoria Executiva da Eletrobras RES-486/2020, de 10/08/2020.

Repositório

Os regulamentos das empresas Eletrobras podem ser encontrados nas redes de *intranet* das empresas.

Direitos de autor e confidencialidade

Prazo máximo de revisão: 3 anos.

Histórico de edições: não se aplica.

Sumário

Capítulo I – Geral

Seção I – Introdução

Objetivo

Estabelecer diretrizes para a governança de privacidade e de proteção dos dados pessoais, visando à gestão do tratamento de dados pessoais e à gestão de incidentes de segurança da informação, no ambiente convencional ou de tecnologia das empresas Eletrobras, com o propósito de proteger a privacidade de consumidores, colaboradores, parceiros ou fornecedores.

Abrangência

Este regulamento dispõe sobre a governança da privacidade e da proteção de dados pessoais, no âmbito das Empresas Eletrobras sediadas em território nacional.

Referências legais e institucionais

Foram utilizadas as seguintes referências legais e institucionais na elaboração deste regulamento:

a) Lei nº 12.527/2011, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI) – Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

b) Lei nº 12.813/2013, de 16 de maio de 2013 (Lei de Conflito de Interesses) – Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego.

c) Lei nº 12.965/2014, de 23 de abril de 2014 (Marco Civil da *Internet*) – Estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil.

d) Lei nº 13.460/2017, de 26 de junho de 2017 – Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

e) Lei nº 13.709/2018, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) – Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da *Internet*).

f) Lei nº 13.853/2019, de 8 de julho de 2019 – Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados.

g) Lei nº 14.010/2020, de 10 de junho de 2020 – Altera a data de entrada em vigor dos arts. 52, 53 e 54 da Lei nº 13.709, de 14 de agosto de 2018.

h) Decreto nº 8.771/2016, de 11 de maio de 2016 – Regulamenta a Lei nº 12.965/2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na *internet* e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

i) Decreto nº 9.492/2018, de 5 de setembro de 2018 – Regulamenta a Lei nº 13.460, de 26 de junho de 2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública federal, institui o Sistema de Ouvidoria do Poder Executivo Federal.

j) Decreto nº 9.637/2018, de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação.

k) Decreto nº 10.153/2019, de 3 de dezembro de 2019 – Dispõe sobre as salvaguardas de proteção à identidade dos denunciantes de ilícitos e de irregularidades praticados contra a administração pública federal direta e indireta.

l) Política de Gestão de Documentos e Informações Corporativas das Empresas.

m) Plano de Classificação de Documentos das Empresas Eletrobras.

n) Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras.

o) Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras.

p) Normativo de gestão de consequências das empresas Eletrobras.

q) Arquitetura de Processos das Empresas Eletrobras.

r) Código de Conduta Ética e Integridade das Empresas Eletrobras.

Seção II – Diretrizes

Subseção I – Gerais

Artigo 1º – Este regulamento é aplicado a todos os colaboradores das empresas Eletrobras que realizem atividades que envolvam, de forma direta ou indireta, o tratamento de dados pessoais.

Artigo 2º – A governança de privacidade e dados pessoais das empresas Eletrobras deve ser pautada na relação de confiança com os titulares de dados pessoais, por meio de atuação transparente, com monitoramento contínuo e avaliações periódicas integradas à sua estrutura geral de governança.

Artigo 3º – A identificação dos tratamentos de dados pessoais nas empresas Eletrobras deve ser orientada por processos, tendo como base a Arquitetura de Processos das Empresas Eletrobras.

Artigo 4º – As adequações dos processos, inclusive em seus sistemas, formulários e procedimentos, são de responsabilidade das respectivas áreas de negócio e devem contar com apoio técnico do Encarregado pelo Tratamento de Dados Pessoais (DPO).

Artigo 5º – As adequações dos processos devem ter uma abordagem sistemática que se apoie em padrões e adote condutas de privacidade, de forma proativa e consistente, na aplicação em tecnologias da informação, práticas organizacionais, *design* de produtos ou redes de informação.

Artigo 6º – Os incidentes relacionados a violação de privacidade ou que gerem danos aos titulares de dados pessoais devem ser encaminhados para o DPO de cada empresa, que deve realizar o tratamento de acordo com o Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras.

Subseção II – Tratamento de Dados Pessoais

Artigo 7º – As empresas Eletrobras devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente no caso de tratamento baseado no legítimo interesse ou quando envolver dados pessoais sensíveis. Tal registro deve se dar por meio do documento intitulado Registro de Tratamento de Dados Pessoais (RTD), que deve ser preenchido pelas áreas responsáveis pelas atividades que envolvam tratamento de dados e arquivados pelo DPO de cada empresa.

Artigo 8º – Os tratamentos dos dados pessoais devem observar os seguintes princípios: finalidade, adequação, necessidade, qualidade dos dados, transparência, segurança, prevenção, livre acesso, não discriminação, responsabilização e prestação de contas.

Artigo 9º – Os tratamentos dos dados pessoais podem ser realizados somente mediante enquadramento em uma das bases legais previstas no artigo. 7º da LGPD. No caso de dados pessoais sensíveis, deve considerar o rol mais restritos de bases legais, previstas no artigo 11 da LGPD.

Artigo 10 – Em caso de realização de tratamento baseado no fornecimento de consentimento pelo titular, devem ser observadas as condições para obtenção, previstas no artigo 8º da LGPD: deve ser expresso, claro e destacado de outras cláusulas envolvidas na atividade/serviço, livre de vícios e possuir finalidades determinadas.

Artigo 11 – O término do tratamento de dados pessoais ocorrerá sempre que a finalidade de tratamento for alcançada, por determinação da ANPD, ou mediante solicitação do titular de dados.

Artigo 12 – Os dados pessoais devem ser eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades. Sua manutenção está autorizada para cumprimento de obrigação legal e regulatória, ou mediante anonimização dos mesmos, descaracterizando-os enquanto dados pessoais.

Artigo 13 – Consideram-se para fins de obrigação legal e regulatória os instrumentos de gestão e preservação documental, como os planos de classificação e as tabelas de temporalidade utilizadas pelas empresas Eletrobras.

Artigo 14 – Quando o tratamento de dados pessoais envolver a obrigação legal de sua difusão em transparência ativa, esses devem ser publicados em formato interoperável e estruturado para o uso compartilhado, em cumprimento ao disposto no artigo 25 da LGPD e previsto no artigo 8º, §3, da Lei nº 12.527/2011, a Lei de Acesso à Informação.

Subseção III – Direitos dos Titulares de Dados

Artigo 15 – As empresas Eletrobras devem dispor, em seus *sites*, de página dedicada ao relacionamento com os titulares de dados, contendo, no mínimo:

a) *link* para a Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras;
b) identidade e informações de contato do DPO indicado pela empresa;
c) Sistema de Demandas do Titular de Dados (*Data Subject Request* – DSR);
d) Sistema de Gerenciamento de *Cookies* do *site*.

Artigo 16 – Os sistemas dedicados a demandas do titular de dados – DSR, citados no artigo 15, devem estar preparados para que os titulares de dados possam exercer seus direitos previstos nos artigos 18 e 19 da LGPD.

Subseção IV – Anonimização e Pseudonimização

Artigo 17 – Sempre que possível e oportuno, as empresas Eletrobras podem fazer uso de técnicas de anonimização de dados pessoais, a fim de impossibilitar a associação entre o dado e seu titular, fazendo com que os dados deixem de ser considerados pessoais. A anonimização não pode ser passível de reversão.

Artigo 18 – A anonimização dos dados pessoais pode ser utilizada para permitir a manutenção dos dados do titular, mesmo após o término da finalidade do tratamento.

Artigo 19 – Sempre que possível e oportuno, as empresas Eletrobras podem fazer uso de técnicas de pseudonimização, com o objetivo de minimizar os riscos e danos ao titular, em caso de algum incidente de violação de dados pessoais.

Artigo 20 – As áreas das empresas Eletrobras dedicadas ao tratamento de denúncias podem utilizar técnicas de pseudonimização, buscando reforçar as medidas de proteção dos dados de denunciantes, em alinhamento com o disposto no artigo 6º, §4º, do Decreto nº 10.153/2019.

Artigo 21 – As ouvidorias das empresas Eletrobras podem usar técnicas de pseudonimização para proteger a identidade de autor de manifestação, conforme previsão do art. 24 do Decreto nº 9.492/2018.

Subseção V – Governança dos Riscos

Artigo 22 – Os riscos gerados para as empresas Eletrobras, em razão da LGPD, devem ser gerenciados e priorizados por meio de eventos e fatores de riscos na Matriz de Riscos das Empresas Eletrobras.

Artigo 23 – A gestão de riscos para os titulares de dados, gerada a partir dos tratamentos de dados identificados nas empresas Eletrobras, deve utilizar o RTD, que contém identificação, análise e avaliação dos riscos, e o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que contém as medidas de respostas aos riscos.

Artigo 24 – Os RTDs e os RIPDs devem ser revisados anualmente, ou sempre que houver qualquer mudança no tratamento do dado pessoal.

Artigo 25 – Caso os tratamentos sejam baseados no legítimo interesse do controlador/operador, envolvam dados pessoais sensíveis ou ainda gerem riscos às liberdades civis e aos direitos fundamentais do titular, deve ser elaborado o RIPD, com o objetivo de identificar medidas, salvaguardas e mecanismos de mitigação de risco.

Parágrafo único – Todo RIPD deve ter, como anexo, o RTD correspondente.

Seção III – Responsabilidades

Artigo 26 – **O Conselho de Administração da Eletrobras deve:** deliberar sobre as diretrizes estratégicas da governança de proteção de dados pessoais.

Artigo 27 – **A Diretoria Executiva da Eletrobras deve:** indicar, no âmbito da *holding*, o Encarregado pelo Tratamento de Dados Pessoais (DPO).

Artigo 28 – **As diretorias executivas das empresas Eletrobras devem:** indicar, na respectiva empresa, o DPO.

Artigo 29 – **O Encarregado pelo Tratamento dos Dados Pessoais da Eletrobras (*DPO)* deve:**

a) Aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar providências.

b) Receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências.

c) Orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

d) Orientar as áreas responsáveis pelo processo/atividade que leva ao tratamento dos dados na elaboração do RTD e do RIPD.

e) Orientar os encarregados de tratamento dedados das empresas Eletrobras na execução de suas atribuições.

f) Executar as demais atribuições determinadas pela Eletrobras ou estabelecidas em normas complementares.

g) Manter este regulamento atualizado.

Artigo 30 – **Os Encarregados pelo Tratamento dos Dados Pessoais das Empresas Eletrobras (DPOs) devem**:

a) Aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar providências.

b) Receber comunicações da autoridade nacional e adotar providências.

c) Orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

d) Orientar as áreas responsáveis pelo processo/atividade que leva ao tratamento dos dados na elaboração do RIPD.

e) Executar as demais atribuições determinadas pela respectiva empresa ou estabelecidas em normas complementares.

f) Colaborar, junto ao DPO da Eletrobras, na atualização deste regulamento.

Artigo 31 – **As áreas de tecnologia da informação das empresas Eletrobras devem:**

a) Assegurar que os sistemas sejam projetados, desde a sua concepção, para que a coleta e o tratamento de dados pessoais estejam limitados ao propósito identificado e declarado.

b) Garantir o descarte de dados pessoais temporários e dos dados pessoais, que estiverem em formato digital, após o término do tratamento.

c) Garantir a anonimização dos dados pessoais, quando necessária sua manutenção para além da finalidade original.

d) Garantir o controle de acesso aos dados pessoais, bem como primar por sistemas que possam realizar auditoria de *log* e rastreabilidade do fluxo dos dados.

Artigo 32 – **Os gestores das áreas responsáveis pelo processo/atividade que leva ao tratamento dos dados nas empresas Eletrobras devem:**

a) Viabilizar ao titular de dados, com apoio da área de TI e orientação do DPO, mecanismos que permitam a revogação do consentimento a qualquer momento, mediante manifestação expressa.

b) Elaborar RTD, de acordo com o artigo 7º deste regulamento.

c) Elaborar RIPD, de acordo com o artigo 25 deste regulamento, com orientação do DPO.

d) Atender às demandas do DPO e das áreas de segurança da informação, acerca dos dados sob sua responsabilidade.

Artigo 33 – **As áreas responsáveis pela segurança da informação nas empresas Eletrobras devem:**

a) Apoiar o DPO na realização de suas atribuições.

b) Apoiar a realização e a atualização dos RTDs, a partir de informações fornecidas pelas áreas das empresas.

c) Colaborar com a elaboração dos procedimentos para tratamento e resposta a incidentes relativos à privacidade de titulares de dados, de acordo com o Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras.

Artigo 34 – **As áreas de gestão de pessoas das empresas Eletrobras devem:** promover ações de treinamento e desenvolvimento referentes à proteção de dados pessoais e privacidade, de acordo com as solicitações e orientações do DPO.

Artigo 35 – **Os colaboradores devem:**

a) Realizar as ações de treinamentos e desenvolvimento disponibilizadas pela área de gestão de pessoas, referentes à proteção de dados pessoais e privacidade.

b) Cumprir este regulamento, utilizando de forma responsável, profissional, ética e legal as informações corporativas que contenham dados pessoais, respeitando os direitos e a privacidade dos titulares dos dados.

Capítulo II – Procedimentos

Artigo 36 – Este capítulo registra os procedimentos relacionados ao tratamento de dados pessoais e ao atendimento aos diretos dos titulares.

1 Tratamento de Dados Pessoais

1.1 O gestor da área identifica os tratamentos de dados pessoais e elabora o respectivo RTD, conforme o artigo 24 deste regulamento.

1.2 O gestor da área encaminha o RTD ao DPO por meio do *e-mail* específico, definido para este fim em cada uma das empresas Eletrobras.

1.3 O DPO analisa o RTD, propõe ajustes, se necessário, e o reencaminha ao gestor da área.

1.4 O gestor da área realiza os eventuais ajustes necessários e devolve o RTD ao DPO.

1.5 Caso ajustes não sejam necessários, o DPO recebe, assina e arquiva o RTD.

1.6 Caso haja necessidade de preenchimento de RIPD, o DPO encaminha o formulário ao gestor da área.

1.7 O gestor da área preenche o RIPD e o encaminha ao DPO.

1.8 O DPO analisa o RIPD, propõe medidas adicionais, se necessário, e o reencaminha ao gestor da área.

1.9 O gestor da área realiza os ajustes necessários e devolve o RIPD ao DPO.

1.10 Caso novas medidas não sejam necessárias, o DPO recebe, assina e arquiva o RIPD.

1.11 O DPO encaminha o RIPD à ANPD, quando solicitado.

2 Direitos/Demandas dos Titulares de Dados Pessoais

2.1 O titular registra sua solicitação por meio da abertura de demanda nos canais disponíveis nos *sites* das empresas Eletrobras, ou pelos *e-mails* disponibilizados.

2.2 O DPO recebe a demanda e realiza sua verificação, conforme segue:

2.2.1 Se houver sistema específico disponível, pelo qual o titular possa, de maneira autenticada, exercer seus direitos, encaminha *link* e encerra a demanda.

2.2.2 Se não houver sistema disponível para acesso direto do titular, identifica a área responsável pelo tratamento dos dados, solicita ao gestor o envio das informações necessárias, disponibiliza-as ao titular e encerra a demanda.

Capítulo III – Disposições Gerais e Transitórias

Artigo 37 – A Diretoria Executiva da Eletrobras deve aprovar este regulamento e garantir sua implantação.

Artigo 38 – As diretorias executivas das empresas Eletrobras devem garantir a divulgação e a implantação deste regulamento.

Artigo 39 – As ações decorrentes deste regulamento devem estar rigorosamente alinhadas com o Plano Estratégico, o Plano Diretor de Negócio e Gestão, a Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras e a Política de Segurança da Informação das Empresas Eletrobras.

Artigo 40 – As diretrizes estabelecidas neste regulamento devem ser cumpridas por todos os seus destinatários, estando os mesmos sujeitos, no caso de descumprimento, ao estabelecido em normativo específico sobre gestão de consequências.

Artigo 41 – Este regulamento pode ser desdobrado em documentos normativos internos específicos para cada empresa Eletrobras, sempre alinhados aos princípios e diretrizes aqui estabelecidos.

Artigo 42 – As empresas Eletrobras devem adequar a este regulamento os documentos normativos e os controles internos que se fizerem necessários, no prazo máximo de 180 dias a partir da aprovação pela Diretoria Executiva da Eletrobras.

Artigo 43 – Devem ser revogados, em todo ou em parte, os documentos normativos das empresas Eletrobras que estabeleçam diretrizes e procedimentos contrários aos descritos neste regulamento.

Capítulo IV – Glossário

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.

Autoridade Nacional de Proteção de Dados – Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em todo o território nacional.

Colaborador – Diretores, conselheiros, empregados, contratados, prestadores de serviço, estagiários e jovens aprendizes que atuem nas empresas Eletrobras.

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

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

Dado Pessoal – Informação relacionada a pessoa natural identificada ou identificável.

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

DPO (*Data Protection Officer)* – Encarregado pelo Tratamento dos Dados Pessoais – Profissional indicado, em cada empresa, para tratar os incidentes relacionados a violação de privacidade ou que gerem danos aos titulares de dados pessoais e para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Eliminação – Exclusão de dado ou de conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado.

LGPD (Lei Geral de Proteção de Dados Pessoais) – Lei nº 13.709/2018, de 14 de agosto de 2018.

Operador – Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Pseudonimização – Utilização de meios técnicos por meio dos quais 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.

RIPD (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 as medidas, as salvaguardas e os mecanismos de mitigação de risco.

RTD (Registro de Tratamento de Dados) – Formulário que o controlador e o operador devem manter com o registro das operações de tratamento de dados pessoais que realizarem, especialmente no caso de tratamento baseado no legítimo interesse.

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.