Hierarquia dos Documentos

LIVRO DE POLÍTICAS

ECONOMUS

POLÍTICA DE PROTEÇÃO E GOVERNANÇA DE DADOS PESSOAIS

NT 2022/194, de 30.01.2023

1. POLÍTICA DE PROTEÇÃO E GOVERNANÇA DE DADOS PESSOAIS

1.1. Objetivo

1.1.1. Esta Política consolida os princípios e práticas de proteção e governança de dados pessoais adotados pelo Economus, quanto ao tratamento de dados pessoais.

1.2. Abrangência

1.2.1. Esta Política aplica-se a:

a) Conselheiros - membros dos Conselhos Deliberativo e Fiscal do Economus;

b) Dirigentes - membros da Diretoria Executiva do Economus;

c) Empregados - empregados do quadro próprio do Patrocinador;

d) Colaboradores - Terceirizados, Consultores e Jovens Aprendizes;

e) Fornecedores e Prestadores de serviço e seus empregados - enquanto prestarem serviços ao Economus.

1.3. Responsável

1.3.1. A área de Riscos e Controles Internos é a gestora da Política de Proteção e Governança de Dados Pessoais.

1.4. Introdução

1.4.1. A presente Política dispõe sobre os procedimentos que deverão ser observados em todas as atividades que envolvam a coleta, o acesso ou o tratamento de dados pessoais de participantes, beneficiários e seus dependentes, empregados, colaboradores, conselheiros, dirigentes, fornecedores e prestadores de serviço, prepostos do Instituto, bem como de quaisquer outras pessoas físicas cujos dados se tornem acessíveis em razão das atividades realizadas.

1.4.2. O tratamento de dados deve ser realizado assegurando que sejam sempre tratados em observância aos princípios da boa-fé, finalidade, adequação e necessidade, bem como livre acesso, segurança, prevenção e não discriminação, de modo a preservar a transparência ao titular dos dados sobre o tratamento de seus dados pessoais e dados pessoais sensíveis, conforme as melhores práticas de governança e mitigação de riscos.

1.5. Princípios

1.5.1. Todo e qualquer tratamento de dados pessoais e dados pessoais sensíveis no âmbito do Instituto ou mediante solicitação deste, deverá ser realizado de acordo com as regras e procedimentos estipulados em normas relativas à proteção de dados pessoais, e pautadas na boa-fé, lealdade, respeito e transparência ao tratamento dos dados pessoais, e nos seguintes princípios:

a) Adequação: os dados pessoais são tratados em compatibilidade com as finalidades informadas ao seu titular ou pertinentes ao contrato por ele firmado com o Instituto, no contexto do tratamento realizado;
b) Finalidade: os dados pessoais coletados e processados são utilizados para realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, não sendo utilizados de forma incompatível com tais objetivos;
c) Livre acesso: é assegurada aos titulares a realização de consulta facilitada e gratuita sobre os dados pessoais tratados, bem como sobre a forma e a duração do seu tratamento;
d) Não discriminação: é vedada a realização de tratamento de dados pessoais para qualquer forma de discriminação ilícita ou abusiva;
e) Necessidade: o tratamento deve se limitar ao mínimo possível de dados pessoais indispensáveis à realização das finalidades objetivadas, observada a sua pertinência e proporcionalidade;
f) Prevenção: são aplicáveis para tratamento de dados pessoais todas as medidas técnicas, operacionais e contratuais adequadas para prevenir eventual ocorrência de danos ou riscos em virtude das atividades de tratamento de dados pessoais;
g) Qualidade dos dados: os dados pessoais tratados devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade do tratamento;
h) Responsabilização e prestação de contas: é disponível ao titular de dados pessoais a demonstração da adoção de medidas eficazes e capazes de comprovar a observância, o cumprimento e a eficácia das normas de proteção de dados pessoais;
i) Segurança: são aplicáveis para tratamento de dados todas as 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; e
j) Transparência: é assegurado ao titular de dados pessoais o acesso a informações precisas e facilitadas sobre o tratamento de seus dados pessoais e os respectivos agentes de tratamento.

1.6. Do Tratamento de dados pessoais

1.6.1. Todo e qualquer tratamento de dados realizado no âmbito do Instituto, ou a pedido deste, deve ter por preceito mínimo a observância aos princípios indicados nesta Política, mesmo nos casos em que

o tratamento seja baseado em consentimento fornecido pelo titular, para execução de contrato ou procedimentos preliminares ao contrato, cumprimento de obrigação legal ou regulatória, para exercício regular do direito em processo judicial, administrativo ou arbitral, ou em razão do legítimo interesse do Instituto.

1.6.2. Na ocorrência de tratamento com base em legítimo interesse, são requisitos indispensáveis:

a) a proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais;

b) utilização dos dados pessoais estritamente necessários para o atendimento à finalidade pretendida; e

c) adoção das medidas para garantir, ao titular, a transparência do referido tratamento de dados.

1.7. Do tratamento dos dados pessoais sensíveis

1.7.1. O tratamento de dados sensíveis ocorre apenas quando se tornar indispensável para cumprimento de contrato firmado junto ao titular, obrigação legal, regulatória e defesa em processos judiciais, administrativos e arbitrais, em estrita observância às disposições da LGPD, de modo a impedir tratamentos discriminatórios ou restritivos.

1.7.2. Em razão de vedação expressa pela LGPD, o tratamento de dados de saúde não deve ser realizado para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

1.8. Da coleta de dados pessoais

1.8.1. A coleta de dados pessoais deve ser destinada a atender propósitos específicos e legítimos, observada limitação aos dados pessoais mínimos necessários para atendimento às respectivas finalidades, de modo a assegurar que:

a) o titular dos dados pessoais seja informado em contrato, e-mail ou pessoalmente, de maneira clara e específica sobre como seus dados serão tratados e para quais finalidades;

b) o tratamento é adequado ao contexto em que os dados pessoais foram coletados; e

c) a indispensabilidade dos dados pessoais coletados para atingir aquela finalidade pretendida.

1.9. Dados pessoais de crianças e adolescentes

1.9.1. Na coleta de dados pessoais de menores de 18 (dezoito) anos, inclusive dos beneficiários dos planos de previdência e saúde e seus dependentes e/ou dos dependentes de colaboradores, empregados, conselheiros e dirigentes do Instituto, deverão ser adotados procedimentos para certificar que a coleta de dados e o consentimento para o tratamento de dados é realizado diretamente pelos pais ou responsáveis legais, quando aplicável.

1.9.2. Observada a legislação que rege a operação de saúde e as informações necessárias para operacionalização do escopo dos contratos firmados com o Instituto, dados pessoais de beneficiários dependentes maiores de 17 (dezessete) anos não poderão ser disponibilizados a terceiros.

1.10. Do compartilhamento de dados pessoais

1.10.1. O compartilhamento de dados pessoais pelo Instituto é classificado em três níveis, de acordo com a categoria e a confidencialidade dos dados, bem como o enquadramento do tratamento realizado:

a) compartilhamento amplo, quando se tratar de dados públicos ou tornados manifestamente públicos pelo titular, que não estão sujeitos a restrição de acesso e compartilhamento, resguardados os diretos do titular dos dados e os princípios estabelecidos nesta Política e na LGPD;

b) compartilhamento restrito, quando se tratar de dados pessoais coletados ou disponibilizados para o cumprimento de contrato e seus procedimentos preliminares ou para o cumprimento de obrigação legal ou regulatória;

c) compartilhamento específico, quando se tratar de compartilhamento de dados confidenciais, sigilosos, dados sensíveis e dados de crianças e adolescentes;

1.10.2. O compartilhamento de dados ocorrerá com base no disposto nos itens 1.11 e 1.12 desta Política, devendo, o receptor dos dados, garantir o adequado tratamento e segurança dos dados pessoais recepcionados.

1.10.3. O compartilhamento de dados pessoais com base no legítimo interesse do controlador enquadra-se em compartilhamento específico de dados, devendo, nestes casos, o tratamento e compartilhamento serem precedidos de comunicação prévia ao DPO, com observância aos preceitos contidos no item 1.7 desta Política.

1.11. Dos cuidados no compartilhamento de dados pessoais

1.11.1. As disposições gerais deste item são aplicáveis em qualquer hipótese de compartilhamento de dados pessoais pelo Instituto ou pelos fornecedores e parceiros, independentemente do enquadramento de categoria.

1.11.2. O compartilhamento de dados pessoais pelo Instituto deve ocorrer apenas quando houver consentimento do seu titular ou quando seja necessário à realização do tratamento previamente autorizado pelo titular, inclusive por decorrência de contratos firmados com o Instituto, na operacionalização das atividades dos planos de previdência e assistenciais administrados, ou quando indispensável para cumprimento de finalidade cuja atividade de tratamento de dados está pautada em base legal diversa autorizada pela LGPD.

1.11.3. Os contratos e convênios com terceiros, para os quais haja o compartilhamento de dados pessoais, devem conter cláusulas específicas dispondo sobre a observância à proteção e governança de dados pessoais e medidas de minimização de riscos.

1.12. Do compartilhamento de dados sensíveis

1.12.1. O compartilhamento de dados pessoais sensíveis é permitido nas seguintes hipóteses, com a devida observância às disposições do item 1.11 desta Política:

a) para possibilitar, ao seu beneficiário e seus dependentes, a prestação de serviços assistência à saúde, nos termos contratados;

b) portabilidade de dados quando consentido pelo titular;

c) a realização de transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde e assistência à saúde;

d) guarda externa de documentos perante empresa contratada;

e) para cumprimento de obrigações regulatórias;

f) defesa em processos judiciais e administrativo; e

g) quando devidamente consentido pelo titular.

1.13. Da transferência internacional

1.13.1. Nos casos em que se fizer necessária a realização de transferência internacional de dados pessoais, inclusive por fornecedores que atuam em nome do Economus, deve ser previamente verificada a existência, no país de destino, de norma ou dever de proteção de dados pessoais, em observância ao fiel cumprimento das disposições e requisitos estabelecidos nesta Política e na LGPD, com a

formalização de cláusula contratual específica para determinação de condições para transferência internacional realizada por fornecedores.

1.14. Eliminação de dados pessoais

a) O tratamento e armazenamento de dados pessoais somente estão autorizados pelo período necessário à realização das finalidades que motivaram a coleta e tratamento de tais dados, bem como para cumprimento de obrigações contratuais e legais, observada a sua indisponibilidade, quando do término do tratamento, em sistemas, redes ou pastas físicas do Instituto;

b) Os dados pessoais e dados pessoais sensíveis tratados pelo Instituto devem ser mantidos enquanto existir relação jurídica com o respectivo titular, exceto nos casos em que, por observância à legislação ou regulamentação, seja necessária a conservação por prazo superior, findo o qual os dados pessoais e os dados pessoais sensíveis serão eliminados;

c) A eliminação de documentos contendo dados pessoais deverá seguir o procedimento especificado na tabela de temporalidade do Instituto; e

d) Havendo determinação por parte de autoridade pública ou judicial para a manutenção de informações relacionadas a pessoas físicas, o Economus deverá atender ao mandamento, procedendo com a exclusão após passado o período determinado.

1.15. Data Protection Officer - DPO (Encarregado)

1.15.1. O DPO indicado como responsável pelo canal de comunicação entre o Instituto, os titulares de dados pessoais (participantes, beneficiários e seus dependentes, colaboradores, empregados, fornecedores e prestadores de serviço, dirigentes, conselheiros e prepostos), partes interessadas e a Autoridade Nacional de Proteção de Dados (ANPD), deve prestar os esclarecimentos necessários sobre esta Política e sua aplicação, casos excepcionais e boas práticas a serem adotadas permanentemente por empregados, colaboradores, conselheiros, dirigentes, fornecedores, prestadores de serviço e parceiros do Instituto.

1.15.2. São atribuições legais do DPO:

I. aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II. receber comunicações da autoridade nacional e adotar providências;

III. orientar aos que esta política abrange, conforme descrito no item 1.2.1., a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV. executar as demais atribuições determinadas pelo Instituto ou estabelecidas em normas complementares.

Para atendimento aos itens (III) e (IV), o DPO deverá estar diretamente envolvido nas ações de governança de dados pessoais previstas na LGPD, tais como:

a) identificar processos/operações envolvendo dados pessoais, bem como sua permanente atualização, observado o enquadramento legal quanto a bases para tratamento, finalidade, necessidade e adequação e eventual existência de transferência internacional de dados pessoais;

b) definir mecanismos para assegurar transparência e livre acesso de dados pessoais pelos titulares de dados, especialmente para atendimento aos direitos mínimos;

c) estabelecer providências para manutenção da qualidade dos cadastros, atendimento a requisitos específicos para dados pessoais de menores e eventual minimização ou anonimização de dados;

d) identificar medidas de segurança, técnicas e administrativas, para prevenção a acessos não autorizados, danos aos titulares e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados pessoais;

e) gestão da temporalidade do armazenamento de dados pessoais, tanto nos ambientes físicos como eletrônico/digital;

f) conduzir obrigações atribuíveis ao Economus na qualidade de controlador de dados, como elaboração relatório de impacto de proteção de dados pessoais, definição das condições tratamento e dados pelos operadores, inclusive cláusulas contratuais, registro das operações de tratamento de dados pessoais e gestão de incidentes de segurança;

g) identificar e monitorar riscos relacionados à proteção de dados pessoais; e

h) implementar programa de governança em privacidade que contemple políticas, boas práticas monitoramento contínuo e avaliações periódicas.

1.15.3. O DPO deve ainda, como boa prática, participar das questões que envolvam proteção de dados pessoais, ter recursos para o desempenho da função e executar a atividade com independência e sem conflito de interesses.

1.15.4. Eventuais incidentes de vazamentos ou riscos de exposição de dados pessoais tratados pelo Instituto deverão ser reportados ao DPO com a máxima brevidade possível, conforme procedimentos descritos em Plano de Resposta a Incidentes do Economus.

1.16. Direitos dos titulares e canal de gerenciamento de solicitações

1.16.1. É assegurado o acesso facilitado e claro às informações sobre o tratamento de dados pessoais realizados pelo Instituto, sempre que solicitado pelo titular dos dados, em alinhamento às recomendações de autenticação e workflow de tratativas previstas na Política/Manual de Atendimento do Economus.

1.16.2. As solicitações relativas aos direitos de privacidade e proteção de dados dos titulares deverão ser efetuadas e encaminhadas ao canal de gerenciamento de solicitações, conduzido pelo DPO.

1.17. Relatório de impacto à proteção de dados pessoais

1.17.1. Nos casos em que o tratamento de dados oferecer riscos às liberdades civis e aos direitos fundamentais do titular, deve ser previamente verificada elaboração de relatório de impacto à proteção de dados pessoais, contendo a descrição dos processos de tratamento de dados pessoais e as medidas, salvaguardas e mecanismos de mitigação de risco adotados, observando o modelo de avaliação de riscos utilizado pelo Economus.

1.18. Privacidade desde a concepção

1.18.1. A todo projeto ou operação desenvolvido pela ou sob demanda do Instituto, incluindo novos planos, o desenvolvimento de aplicações, hardware ou software, iniciativas de comunicação e relacionamento e demais processos internos, devem ser incorporados os conceitos e práticas de privacidade desde a concepção, para garantia da governança e proteção dos dados pessoais do usuário.

1.19. Das Ações Preventivas

O Economus promove e incentiva, de forma contínua, a ocorrência de práticas concretas e ações preventivas para a conscientização e concretização das diretrizes de segurança, privacidade e proteção de dados pessoais, conforme a seguir indicado:

a) Canal interno de dúvidas e sugestões para o público de abrangência desta Política

Utilização da Comissão de Privacidade e Proteção de Dados como canal interno para atender às dúvidas aos que abrangem esta política em procedimentos de tratamento de dados pessoais, a fim de garantir a adoção das melhores práticas em procedimentos e operações da entidade.

b) Capacitação

Promoção de ações de educação para seus conselheiros, diretores, colaboradores, empregados e fornecedores, para a conscientização sobre procedimentos de segurança da informação, envolvendo treinamentos, palestras, dentre outros.

c) Comunicação interna

Amplo canal de comunicação aos que abrangem esta política via newsletter, informativos na sede da entidade, vídeos institucionais e demais ações de divulgação de boas práticas sobre procedimentos de segurança da informação englobando cuidados da proteção de dados pessoais.

d) Gestão documental e exclusão/minimização de dados pessoais

Revisão dos procedimentos de gestão documental do Economus, com a política de retenção e eliminação de dados pessoais dispondo sobre diretrizes aplicáveis aos casos de eliminação de dados pessoais ao término do tratamento ou a minimização de tais dados nos suportes/sistemas.

A este respeito, tem-se que o descarte de papéis contendo dados pessoais deverá ser precedido de fragmentação, de modo a assegurar a não divulgação do seu conteúdo nas etapas de exclusão.

e) Interface com terceiros

Implementação de cuidados específicos na interface com terceiros, inclusive os patrocinadores e fornecedores que atuam como operadores de dados pessoais em nome do Economus, com a formalização de contratos, termos ou convênios dispondo sobre a observância à proteção e governança de dados pessoais e medidas de minimização de riscos, bem como expressa manifestação, sempre que aplicável, sobre a aderência às exigências legais e a indicação de quais as providências foram ou estão sendo adotadas pelo fornecedor para cumprimento das orientações de proteção de dados pessoais e mitigação de riscos inerentes, inclusive, mas não somente, no tocante a:

I. medidas organizacionais e administrativas visando garantir cultura de privacidade e proteção de dados;

II. mecanismos internos de supervisão, de mitigação de riscos, normas de segurança e padrões técnicos destinados a dar segurança ao processo de tratamento de dados com o fim de evitar incidentes de segurança;

III. providências de natureza técnica e organizacional necessárias para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado, bem como contra qualquer forma de tratamento ilícito ou irregular;

IV. acesso a dados pessoais e ou dados sensíveis estritamente necessários e exclusivamente para atendimento às finalidades do contrato mantido;

V. atendimento às bases legais previstas na LGPD para tratamento de dados pessoais e ou dados pessoais sensíveis, conforme o caso;

VI. eliminação de dados pessoais após o término de seu tratamento, no âmbito e nos limites técnicos das atividades objeto do contrato, observada a conservação nas hipóteses autorizadas por lei;

VII. adequação dos processos e atividades que envolvam transferência internacional de dados às condições previstas na LGPD;

VIII. manutenção de registro das operações de tratamento de dados pessoais que realizarem, inclusive quando baseado no legítimo interesse; e

IX. atendimento de requisitos de segurança nos sistemas utilizados

Os canais utilizados para tráfego de dados pessoais deverão ser seguros, quer por meio da limitação de acesso via portal próprio do fornecedor/operador ou da entidade, FTP ou uso de senhas e técnicas de criptografia, observado volume e sensibilidade dos dados pessoais compartilhados.

f) Mapeamento e controle de risco

Mapeamento e controle dos riscos em que a entidade possa estar exposta relativamente à LGPD, com a inclusão de apontamentos específicos na matriz de risco e seu tratamento, bem como ferramentas de gestão do risco e da sua aderência às práticas.

Para tanto, são cabíveis medidas de medição ou teste de vulnerabilidades, ameaças e riscos cibernéticos ou externos, bem como controle de acesso a sistemas, rede corporativa e área restrita do site, além de arquivos físicos que contenham dados pessoais.

g) Políticas e normativos internos

Revisão de políticas e normativos internos para adequação às diretrizes e cuidados de proteção de dados pessoais, bem como a manutenção de parâmetros a serem seguidos pelos colaboradores e os profissionais que agem em nome do Economus, inclusive fornecedores.

h) Redução do trâmite de papel:

Adoção de procedimentos para reduzir o uso de papel nas atividades do Economus, buscando a redução dos riscos de eventual extravio, perda, dano ou vazamento de documentos que contenham dados pessoais, e custos financeiros (malotes, correios, tempo de colaboradores para transporte de documentos, armazenamento interno e externo).

Poderão ser adotadas ferramentas alternativas de trabalho (multiplicidade de monitores, entre outros) e de estímulo à redução do papel por meio de metas, premiações, fiscalização de mesas ou outro.

i) Registro das atividades com dados pessoais

Registro das atividades desenvolvidas pelo Economus envolvendo dados pessoais, devidamente documentado por meio de relatórios, fluxos e inventários de dados pessoais, arquivos magnéticos (gravação de voz, tela ou outro), registros de atendimento e instrumentos contratuais com operadores de dados pessoais em todos os processos para evidenciar a adequação de procedimentos à proteção de dados pessoais e subsidiar eventual elaboração de Relatórios de Impacto à Proteção de Dados Pessoais, quando aplicável.

j) Resolução de conflitos

Adoção de procedimentos para a criação de um ambiente de mediação de conflitos decorrentes de incidentes de vazamento ou exposição indevida de dados, preferencialmente por meio de plataforma de mediação online, para propiciar uma célere resolução entre o titular de dados e o Economus.

k) Revisão dos formulários e instrumentos

Revisão dos formulários e instrumentos específicos que envolvem a coleta de dados pessoais de participantes e assistidos, para adequação à LGPD, especialmente quanto à necessidade, finalidade, adequação, qualidade, livre acesso, transparência e não discriminação.

l) Sistema de gerenciamento de solicitações externas

Criação de processo interno, mediado pelo encarregado, de recepção e gerenciamento e respostas a solicitações externas, feitas por terceiros, sobre o possível tratamento indevido de dados.

1.20. Glossário

1.20.1. Para efeitos desta Política, são considerados os seguintes termos e seus respectivos significados:

a) Agentes de tratamento de dados - controlador, pessoa natural ou jurídica, de direito público ou privado, a quem compete a tomada de decisões referentes ao tratamento de dados pessoais, e o operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome ou a pedido do controlador;

b) Autoridade Nacional de Proteção de Dados (ANPD) - órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD;

c) Dado pessoal - informação que, isolada ou associada a outras, identifique ou que possa identificar uma pessoa natural;

d) 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;

e) Dado pseudonimizado - informação sobre um titular de dados que somente o identifica quando associada à informação adicional relativa ao titular, mantida separadamente pelo controlador em ambiente controlado e seguro;

f) Encarregado (ou Data Protection Officer - DPO) - pessoa indicada pelo controlador ou operador encarregado para atuar como canal de comunicação com titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD);

g) Titular dos dados pessoais - pessoa natural a quem se referem os dados pessoais e dados pessoais sensíveis que são objeto de tratamento, inclusive participantes, assistidos, beneficiários e dependentes dos planos, colaboradores, dirigentes, fornecedores – quando pessoas físicas - e demais prepostos do Instituto; e

h) Tratamento de dados pessoais - operação realizada com dados pessoais, que abarca 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 de dados pessoais.

1.21. Referências Legais e Normativas

1.21.1. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;

1.21.2. Guia Referencial da Lei Geral de Proteção de Dados para Entidade Fechadas de Previdência Complementar – ABRAAP, maio de 2019;

1.21.3. Resolução Normativa ANS nº 443 de 25 de janeiro de 2019; e

1.21.4. Manual de Adaptação das Autogestão à LGPD – UNIDAS, outubro de 2019.

1.22. Histórico de Atualização

Versão	Data	Nota Técnica	Descrição das Alterações	Próxima atualização
01	06.10.2020	GEGOV/RISCO – 2020/137	criação da política	Até 06.10.2022
02	30.01.2023	GEGOV/RISCO – 2022/194	revisão e atualização	Até 30.01.2025