Norma

006 - Gestão e Privacidade de Dados Pessoais

Revisão: 03 Ano: 2025 - Vigência: 04/08/2025

Próxima Revisão: 04/08/2027

CP - Compliance

SUMÁRIO

1. OBJETIVO 3

2. ABRANGÊNCIA 3

3. REFERÊNCIAS 3

4. DEFINIÇÕES 4

5. RESPONSABILIDADES 6

6. DIRETRIZES GERAIS E ESPECÍFICAS 9

6.1 DIRETRIZES GERAIS 9

6.2 DIRETRIZES ESPECÍFICAS 9

7. MEDIDAS DISCIPLINARES 21

8. CONFIDENCIALIDADE 21

9. APROVAÇÕES 21

10. HISTÓRICO DE REVISÕES 22

1. OBJETIVO

Estabelecer as diretrizes para o sistema de gestão corporativo e tem por finalidade reforçar o compromisso da VEXIA com a sociedade, garantindo que todas as etapas das suas atividades desempenhadas estejam em consonância com a Lei Geral de Proteção de Dados Pessoais.

A VEXIA reconhece a importância da privacidade do ser humano e está comprometida com os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, quando do processamento de dados pessoais.

2. ABRANGÊNCIA

Aplica-se a todos os tratamentos de dados pessoais de fornecedores, parceiros de negócios, funcionários, acionistas, investidores e outros indivíduos pessoa física, realizados pela VEXIA e indica as diretrizes que deverão ser seguidas, seja quando da atuação como Controlador, seja quando da atuação como Operador, tanto no meio digital, quanto no meio físico.

A VEXIA, enquanto Controladora, realiza o tratamento de dados pessoais de seus empregados, terceiros e de usuários do site.

A VEXIA, quando atuar como Operadora, nas atividades de outsourcing, realizando o tratamento de dados pessoais contidos em documentos de diversas naturezas, procederá sempre conforme as instruções formalizadas pelos Controladores, ora Clientes.

Esta Norma aplica-se à VEXIA e suas subsidiárias integrais, controladas direta ou indiretamente, que conduzem negócios no âmbito Nacional e/ou Internacional.

3. REFERÊNCIAS

REFERÊNCIAS EXTERNAS

- Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018).
- Enunciado CD/ANPD nº 1, de 22 de maio de 2023
- Resolução CD/ANPD nº 18, de 16 de julho de 2024

- Resolução CD/ANPD nº 19, de 23 de agosto de 2024
- ABNT NBR ISO/IEC 27001:2022

REFERÊNCIAS INTERNAS

- Política de Privacidade do Site
- 001 - POL - CS - Segurança da Informação
- 002 - NOR - I - CS - Classificação e Tratamento da Informação
- 006 - NOR - I - AR - Controle de Acesso
- 009 - NOR - I - CS - Seg Info - Descarte e Reutilização de Ativos
- 018 - NOR - I - AR - Segurança da Informação - Gestão de Ciclo de Vida dos Dados Pessoais
- 023 - NOR - I - AR - Segurança da Informação - Gerenciamento de Incidentes e Vazamento de Dados

4. DEFINIÇÕES

4.1. **Agentes de tratamento:** o Controlador e o Operador.

4.2. **Anonimização:** Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento para transformar dados pessoais em dados anônimos. Isso significa que o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Assim, a anonimização torna os dados pessoais irreconhecíveis de forma irreversível, impossibilitando a identificação, por meio de tempo, custo e tecnologia razoáveis. Os princípios de processamento de dados pessoais não se aplicam a dados anônimos, pois não são mais dados pessoais.

4.3. **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

4.4. **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

4.5. **Ciclo de Vida:** conjunto de etapas de tratamento de dados, incluindo as de coleta, processamento, transferência, armazenamento, término do tratamento e descarte.

4.6. **Colaborador(es):** todos os profissionais que atuam em nome da Vexia, independentemente (i) do cargo, função, atividade, tempo de casa ou local de trabalho. Inclui acionistas, membros do Conselho de Administração e demais comitês, bem como qualquer (ii) da natureza de vínculo (empregatício, prestação de serviços, estatutário ou outro).

4.7. **Comitê de Cyber e Proteção de Dados Pessoais:** equipe indicada pelo Controlador para apoiar o DPO no programa e na manutenção das adequações à LGPD.

4.8. **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica.

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

4.10. **Dados Pessoais:** qualquer informação relacionada a uma pessoa natural identificada ou identificável (titular dos dados); é considerada identificável a pessoa natural que possa ser identificada, direta ou indiretamente, em especial por meio de uma informação, como nome, número de identificação, dados de localização, identificadores eletrônicos ou outros elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social.

4.11. **Dados Pessoais Identificáveis**: Trata-se de qualquer informação que identifique ou que possa identificar uma pessoa, tais como: geolocalização, endereço IP (Internet Protocol), placa de automóvel, entre outros.

4.12. **Dados Pessoais Sensíveis:** Trata-se de dados pessoais que são, pela sua natureza, particularmente sensíveis, vez que invadem um nível maior de privacidade do indivíduo, podendo criar riscos significativos para os direitos e liberdades fundamentais. Conforme a legislação, dados pessoais sensíveis são: (i) dados sobre a origem racial ou étnica; (ii) dados sobre a convicção religiosa; (iii) dados sobre a opinião política; (iv) dados sobre a filiação sindical; (v) dados sobre a filiação a organização de caráter religioso, filosófico ou político; (vi) dados referente à saúde ou à vida sexual; (vii) dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

4.13. **Eliminação:** exclusão de dado ou de um conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

4.14. **Encarregado de Tratamento de Dados Pessoais ou "DPO" - Data Protection Officer:** pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

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

4.16. **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.

4.17. **Terceiro(s):** Toda pessoa física ou jurídica que não for Colaborador da Vexia e que seja contratada para auxiliar no desempenho de atividades ou agir em nome, interesse ou benefício desta empresa, tais como representantes, consultores, fornecedores, parceiros de negócios, subcontratados, prestadores de serviços em geral, dentre outros.

4.18. **Titular dos dados pessoais:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, o indivíduo.

4.19. **Tratamento:** Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, 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.

4.20. **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.

5. RESPONSABILIDADES

5.1. Encarregado de Proteção de Dados (DPO)

5.1.1. Aceitar reclamações e comunicações dos titulares de dados pessoais, prestar esclarecimentos e adotar providências;

5.1.2. Receber comunicações da autoridade nacional e adotar as providências necessárias, demandando as áreas internas para o cumprimento;

5.1.3. Orientar, por meio do Comitê de Cyber e Proteção de Dados, os funcionários e os contratados da empresa sobre as práticas a serem tomadas em relação à proteção de dados pessoais; e

5.1.4. Quando necessário ou conforme disposição legal, solicitar ao departamento responsável a elaborações do Relatório de Impacto de Proteção de Dados e validar tal documento;

5.1.5. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;

5.1.6. Avaliar o registro de tratamento de dados sempre que ocorrer algum tipo de alteração no tratamento. Em caso de verificação de inconsistência na análise ou de risco no tratamento, poderá solicitar ao departamento responsável pelos dados a realização de um Relatório de Impacto de Proteção de Dados para o tratamento apontado.

5.1.7. Monitorar a conformidade da VEXIA com a LGPD e por qualquer outra legislação aplicável à proteção dos Dados Pessoais;

5.1.8. Validar os atos do Comitê de Cyber e Proteção de Dados;

5.1.9. Conduzir ações corretivas e preventivas em caso de detecção de alguma não conformidade;

5.1.10. Notificar a ANPD, sem demora injustificada e, quando possível, no prazo de 3 dias úteis, observando as diretrizes da norma de gestão de incidentes (023 - NOR - I - AR - Segurança da Informação - Gerenciamento de Incidentes e Vazamento de Dados), sobre as violações de dados pessoais que importem risco para os direitos e liberdades dos titulares dos dados.

5.2. Comitê de Cyber e Proteção de Dados Pessoais

5.2.1. Realizar encontros quinzenais, com a elaboração de atas;

5.2.2. Elaborar indicadores-chaves de sucesso para avaliar a implementação do programa de proteção de dados, buscando a excelência no tratamento lícito de dados;

5.2.3. Elaborar mecanismo de informação ao titular dos dados quando da coleta de tais informações.

5.2.4. Desenvolver e manter políticas, normas, procedimentos e padrões de conduta sobre a temática e garantir que os dados pessoais são recolhidos legalmente;

5.2.5. Realizar, anualmente, treinamento referente às questões de proteção de dados pessoais, com vista a assegurar o conhecimento por parte dos colaboradores acerca das obrigações que lhes são impostas neste âmbito;

5.2.6. Interagir com os departamentos internos para a resolução de questões legais e técnicas relacionadas a privacidade e proteção de dados;

5.2.7. Investigar e apurar possíveis violações de privacidade de dados, bem como formalizar e tomar as medidas corretivas adequadas em tempo hábil;

5.2.8. Garantir e prestar suporte ao Encarregado de Proteção de Dados para a elaboração dos comunicados aos titulares de dados e a Autoridade Nacional de Proteção de Dados;

5.2.9. Implementar diretrizes e desenvolver o Registro das operações de tratamento de dados pessoais;

5.2.10. Implementar diretrizes e desenvolver o Relatório de Impacto de Proteção de Dados pessoais;

5.2.11. Desenvolver e implementar mecanismo de acesso razoável para permitir que os titulares dos dados possam solicitar correção, eliminação ou transmissão dos seus dados pessoais, se apropriado ou exigido por lei, ou em casos de revogação do consentimento;

5.2.12. Manter o registro das solicitações para corrigir, alterar ou destruir os dados pessoais;

5.2.13. Implementar e garantir que as solicitações dos titulares de dados sejam cumpridas dentro de um prazo de 15 dias, como determina a lei. As demais solicitações serão atendidas em prazo razoável, até que ocorra determinação da Autoridade Nacional de Proteção de Dados (ANPD).

5.2.14. Garantir que os operadores ou outros controladores a quem os dados pessoais tenham sido transmitidos sejam informados, em data hábil, sobre as solicitações de apagamentos, retificações ou outras interações advindas dos direitos do próprio titular dos dados;

5.2.15. Assegurar o cumprimento dos processos conforme as disposições deste documento;

5.2.16. Implementar as melhorias conforme definido neste normativo;

5.2.17. Gerar, medir e analisar os dados relacionados a esse processo;

5.2.18. Fornecer informações necessárias para a análise crítica da gestão e implementar as ações acordadas;

5.2.19. Apurar violação de dados pessoais, suspeita ou real;

5.2.20. Atualizar a Política de Privacidade dos sites e aplicativos a qualquer tempo, sempre que uma alteração significativa ocorrer.

5.3. Departamentos Vexia

5.3.1. Manter atualizado o Registro de Operações de Tratamento de Dados Pessoais.

5.3.2. Elaborar o RIPD, conforme o departamento responsável pelo tratamento.

5.3.3. Informar o titular dos dados pessoais sobre a alteração de finalidade dos dados tratados.

5.4. Usuários da Informação / Colaboradores

5.4.1. É de responsabilidade dos usuários da informação/colaboradores, ler, compreender e cumprir integralmente os termos dessa Norma, bem como as demais normas e procedimentos de proteção de dados pessoais aplicáveis.

5.4.2. Garantir o processamento adequado de dados pessoais conforme prevista na Norma;

5.4.3. Comunicar ao DPO qualquer evento que viole esta Norma ou que represente risco aos dados pessoais.

5.4.4. Notificar o Service Desk sobre quaisquer eventos ou incidentes de segurança, vazamento ou exposição de dados ou Dados Pessoais, confirmados ou suspeitos.

5.4.5. Fornecer informações para as averiguações e investigações sempre que solicitado.

5.4.6. Elaborar o RIPD em conjunto com o Encarregado (DPO), sempre que necessário ou requisitado pela Vexia, por meio do DPO ou Comitê de Cyber e Proteção de Dados;

5.5. Service Desk

5.5.1. Atuar como ponto de contato para notificação de colaboradores e/ ou terceiros sobre incidentes confirmados ou suspeitos de comprometimento de Dados.

5.5.2. Informar imediatamente à área de Segurança da Informação sobre qualquer incidente confirmado ou suspeito de comprometimento de dados, seguindo os processos estabelecidos.

5.6. Segurança da Informação

5.6.1. Notificar o DPO e o Comitê de Cyber e Proteção de Dados Pessoais sobre qualquer incidente de segurança envolvendo Dados Pessoais na Vexia, para que avaliem os impactos no negócio e tomem as decisões apropriadas.

5.6.2. Supervisionar a implementação de controles para mitigar incidentes de segurança, avaliando os impactos eventuais de uma violação de segurança da informação.

5.6.3. Executar procedimentos internos para tratar ou minimizar eventos com potencial de resultar em incidentes ou vazamentos de dados pessoais.

5.6.4. Monitorar possíveis incidentes de segurança com base nos logs de sistemas gerados, quando possível.

5.7. Auditoria e Riscos

5.7.1. Conduzir as inspeções/auditorias internas de processo, inclusive no que diz respeito ao programa de privacidade.

6. DIRETRIZES GERAIS E ESPECÍFICAS

6.1 DIRETRIZES GERAIS

A VEXIA, com base neste normativo, faz campanhas de conscientização e manutenção da sua conduta aos tratamentos de dados pessoais aqui descritos, minimizando os impactos e possíveis riscos a vazamento de dados pessoais, executando medidas técnicas razoáveis de segurança da informação, conforme disposto na ISO/IEC 27.001:2022, minimizando falhas e mitigando os riscos de:

- Vazamento de dados pessoais;
- Perda de dados em trânsito;
- Vazamento de dados pessoais via exportação de dados não autorizados;
- Corrupção de base de dados e ou Servidores de arquivos;
- Contenção contra-ataques cibernéticos;
- Tratamento de dados para finalidade diversa ou em inobservância da legislação.

6.2 DIRETRIZES ESPECÍFICAS

6.2.1. A Vexia está comprometida com a legislação de proteção de dados pessoais em todas as etapas do processamento das informações, garantindo transparência, privacidade e segurança no tratamento dos dados pessoais, sempre respeitando o ciclo de vida das informações (018 - NOR - I - AR - Segurança da Informação - Gestão de Ciclo de Vida dos Dados Pessoais), tanto no meio físico quanto no digital.

6.2.2. A Vexia dispõe de sistemas e equipamentos para garantir a segurança dos dados pessoais tratados, criando e atualizando procedimentos que previnem acessos não autorizados (006 - NOR - I - AR - Controle de Acesso), perdas acidentais e/ ou destruição dos dados pessoais. Além disso, assegura a integridade, a confidencialidade e a relevância dos dados pessoais com base no propósito do processamento. A Vexia também disponibiliza recursos para apoiar a operação e garantir a melhoria contínua do programa de privacidade.

6.2.2.1. A Vexia adota medidas de segurança e salvaguarda para assegurar o tratamento adequado e seguro dos dados, conforme descrito em sua Política de Segurança da Informação (001 - POL - CS - Segurança da Informação).

6.2.3. Quanto à classificação e rotulação das informações, inclusive dados pessoais, a Vexia possui uma norma que esclarece as diretrizes sobre o tema (002 - NOR - I - CS - Classificação e Tratamento da Informação).

6.2.4. Mecanismos de segurança adequados, conforme disposto na ISO/IEC 27.001:2022, são adotados pela Vexia para proteger os dados pessoais contra roubo, uso indevido ou violação.

6.2.5. A garantia do processamento adequado de dados pessoais é responsabilidade de todos que trabalham para ou com a Vexia e que possuem acesso a dados pessoais.

6.2.6. A Vexia realiza treinamentos sobre proteção de dados pessoais para ampliar o conhecimento dos colaboradores e garantir que compreendam suas obrigações e direitos nesse contexto.

6.2.7. Os treinamentos são realizados na admissão dos colaboradores com requalificação bianual.

6.2.8. A Vexia realizará, de forma lícita, os possíveis tratamentos de dados: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

6.2.9. A Vexia, ao tratar dados pessoais de seus colaboradores, clientes, acionistas, fornecedores, usuários dos portais web e sistemas de inteligência artificial, parceiros, contatos comerciais e outros titulares de dados, atuará como Controlador. Nesses casos, os dados coletados poderão incluir:

6.2.9.1. **Informações cadastrais:** nome, data de nascimento, sexo, idade, endereço, número do telefone, endereço de e-mail, número de filhos, informações sobre dependentes, documentos de identificação, vistos, autorização de trabalho, contatos de emergência, estado civil, beneficiários de seguro de vida, fotos ou imagens.

6.2.9.2. **Informações financeiras:** valores da remuneração, benefícios e planos de aposentadoria, conta bancária, plano de compra de ações, ações, despesas de viagem.

6.2.9.3. **Informações empregatícias administrativas:** currículo, formulário do candidato, avaliações, registros de segurança, registros de ausência, prontuário médico, relatório de acidentes, análise de desenvolvimento pessoal, números de identificação oficiais, registro de habilidade, carteira de motorista.

6.2.9.4. **Informações sobre a localização do colaborador:** registro de movimentação interna, via utilização de crachá.

6.2.9.5. **Informações sobre o acesso de sites e detalhes de TI:** identificação dos sites acessados, identificação da máquina utilizada.

6.2.9.6. **Informações comerciais:** executivos de vendas, produto/serviço contratado, quantidades, responsáveis pela gestão/entrega, estrutura organizacional.

6.2.9.7. **Informações de monitoramento e fiscalização**: imagem, voz, geolocalização, IP.

6.2.9.8. **Informações de preferências e localização:** cookies, ID, geolocalização.

6.2.9.9. **Informações Judiciais:** fatos, qualificação processual e as partes interessadas.

6.2.9.10. **Informações de Sustentabilidade/ESG:** stakeholders e censo interno.

6.2.9.11. **Informações de fontes públicas:** informações localizadas e consolidadas a partir de consultas em fontes públicas para preservar a integridade e previr o conflito de interesses nas relações da Vexia com Clientes, Parceiros, Fornecedores e Colaboradores.

6.2.10. Os tratamentos de dados pessoais dos colaboradores da Vexia terão as seguintes finalidades: legítimo interesse, cumprimento de obrigações legais ou regulatórias, execução dos contratos de trabalho, aprendizagem e/ou estágio, tutela da saúde, prevenção a fraude, bem como o exercício regular de direitos em processo judicial, administrativo ou arbitral.

6.2.11. Para atingir a finalidade pretendida, a Vexia priorizará a coleta mínima possível de dados pessoais e, quando necessário, poderá transferi-los para empresas terceiras.

6.2.12. Os colaboradores, acionistas, usuários dos portais web, parceiros, clientes, fornecedores e demais titulares dos dados, quando da coleta de dados pela VEXIA, e **quando necessário legalmente**, serão questionados sobre o consentimento, serão também informados sobre a finalidade do tratamento, bem como sobre as possibilidades de transferência de tais informações com outras empresas.

6.2.13. A coleta de dados pessoais sensíveis pela Vexia estará condicionada ao cumprimento de obrigação legal ou regulatória pelo controlador, ao exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, prevenção a fraude, tutela da saúde ou ao consentimento, de forma específica e destacada, do titular de dados.

6.2.14. A Vexia tem especial preocupação com os direitos das crianças e adolescentes. Por isso, a coleta de dados pessoais de crianças (menores de 12 anos) e de adolescentes (de 12 a 18 anos), estará condicionada, em alguns casos, ao consentimento específico e destacado por pelo menos um dos pais ou pelo responsável legal (artigo 14, § 1º, da LGPD). Em outras situações, estará condicionado ou não a autorização do responsável legal, observando ainda o melhor interesse da criança ou adolescente, mas ocorrerá segundo as demais bases legais de tratamento (artigo 7º e 11º, da LGPD), conforme disposto pelo Enunciado CD/ANPD nº 1, de 22 de maio de 2023.

6.2.14.1. Tais tipos de dados pessoais só serão tratados quando: a) da contratação de menor aprendiz e estagiário; b) do processamento de informações dos dependentes de colaboradores da Vexia; c) da interação com os portais web; d) eventos e campanhas com ou sem o uso de imagem, mas com autorização de um dos pais ou responsável legal.

6.2.14.2. A Vexia deverá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos, seja

através de Política ou Aviso de Privacidade, que deverá ser comunicado antes da coleta.

6.2.15. A Vexia assegura que os dados pessoais serão tratados exclusivamente de acordo com as finalidades para as quais foram originalmente coletados, garantindo a existência de um propósito antes da atividade de coleta.

6.2.15.1. Caso a Vexia precise tratar os dados pessoais coletados para finalidade diferente da original, o departamento que assim o fizer deverá comunicar o titular sobre a mudança, informando a nova finalidade de tratamento, a base legal utilizada, e, se necessário, obtendo o consentimento dos titulares de dados por meio documento claro e conciso, através de formulários internos, eletrônicos ou físicos. A solicitação deverá incluir a finalidade original para a qual os dados foram recolhidos e também a(s) finalidade(s) nova(s) ou adicional(ais). A solicitação também deve detalhar a finalidade inicial, a(s) nova(s) finalidade(s) e o motivo da alteração.

6.2.16. Compete à VEXIA identificar a possibilidade de aplicar o legítimo interesse para o tratamento de dados pessoais. No entanto, tal fundamentação legal será utilizada apenas quando devidamente realizado o Relatório de Impacto à Proteção de Dados Pessoais e autorizado pelo Encarregado.

6.2.17. A VEXIA deverá manter os dados pessoais de forma estruturada, possibilitando o mapeamento e a identificação da sua localização, bem como informações sobre o ciclo de vida.

6.2.17.1. A VEXIA buscará meios para que os dados pessoais armazenados eletronicamente sejam protegidos por senhas e/ou criptografados.

6.2.17.2. Dados pessoais presentes em mídias digitais (CD/DVD/pendrive) ou documentos em papel, serão catalogados e armazenados no Centro de Documentação (CEDOC) da VEXIA, que possui infraestrutura especialmente desenvolvida para evitar possíveis episódios de violação de segurança. A lei exige o mesmo tipo de tratamento concedido ao meio digital.

6.2.17.3. O armazenamento de documentos em papel com dados pessoais nas dependências da VEXIA é realizado por meio de armário chaveado, com infraestrutura especialmente desenvolvida para evitar possíveis episódios de violação de segurança.

6.2.18. A VEXIA deverá manter registro de todas as operações de tratamento de dados pessoais que realizar:

6.2.18.1. Cada departamento da VEXIA será responsável por preencher e manter atualizado o documento intitulado Registro de Operações de Tratamento.

6.2.19. O período de armazenamento e conservação dos dados pessoais varia conforme a finalidade. Existem, no entanto, requisitos legais que obrigam a conservar os dados por um tempo determinado. Caso não haja exigência legal específica, os dados serão armazenados

apenas pelo período necessário para cumprir suas finalidades, conforme prazos definidos na 018 - NOR - I - AR - Segurança da Informação - Gestão de Ciclo de Vida dos Dados Pessoais, que tem como anexo o Registro de Operações de Tratamento.

6.2.19.1. Os principais prazos de armazenamento utilizados pela Vexia são:

Até 1 ano	Prazo de retenção previsto pelo Marco Civil da Internet (Lei nº 12.965/2014).
Até 10 anos	Prazo prescricional da ação revisional - Artigo 205, CC; Prazo prescricional da responsabilidade civil em contratos - Artigo 205, CC; Prazo prescricional civil geral, quando não houver legislação especifica - Artigo 205,CC; Prazo decadencial previdenciário - Artigo 103, Lei 8.213.
Até 2 anos	Prazo prescricional da Relação Trabalhista - Artigo 11, da CLT c/c artigo 7º, XXIX, da CF.
Até 20 anos	Conforme prazo definido pela NR 07 em relação aos documentos de saúde ocupacional.
Até 3 anos	Prazo prescricional para cobrar indenização pelos danos causados à imagem - Artigo 206, parágrafo 3º, inciso V, CC.
Até 5 anos	Prazo prescricional das penalidades da Lei Anticorrupção - Artigo 25, Lei 12.813/2023;

	Prazo prescricional da Relação Trabalhista - Artigo 11, da CLT c/c artigo 7º, XXIX, da CF; Prazo prescricional fiscal - Artigos 173 e 174, CTN; Prazo de retenção de prontuários médicos - De acordo com a Resolução nº 1.821/2007 do Conselho Federal de Medicina (CFM), os prontuários médicos devem ser mantidos por um período mínimo de 5 anos a partir da data do último atendimento. Este prazo se refere ao período em que os documentos devem estar disponíveis para consulta.
8 anos	Prazo prescricional para apuração de improbidade administrativa - Artigo 23, Lei nº 8.429/1992.
Enquanto existir o Consentimento	Artigo 18, da LGPD
Indeterminado	Quando se tratar de informações que compõe o histórico empresarial, a manutenção por tempo indeterminado se faz necessária; Quando tratar-se de tema que envolve obrigações de fazer no trabalhista, visto que são imprescritíveis conforme interpretação do artigo 11, §1º da CLT. Dessa forma, dados de colaboradores

	devem ser mantidos por prazo indeterminado; Questões ambientais, isto porque, o prazo prescricional para responsabilidade de danos ambientais é imprescritível conforme entendimento do STF (Recurso Extraordinário (RE) 1427694, com repercussão geral (Tema 1.268)); Histórico e responsabilidade sobre projetos, lembrando que a ABNT NBR 6118 define o prazo mínimo de 50 anos para a vida útil do projeto de estruturas.

6.2.19.2. O prazo de retenção de cada fluxo operacional foi definido com base no prazo prescricional da atividade e encontra-se registrado no Registro de Operações de Tratamento.

6.2.20. O término do tratamento e, consequentemente, o descarte definitivo dos dados pessoais observará a norma de descarte seguro dos dados (009 - NOR - I - CS - Seg Info - Descarte e Reutilização de Ativos) e ocorrerá nas seguintes situações:

6.2.20.1. A finalidade do tratamento foi alcançada.

6.2.20.2. O prazo para o tratamento do dado especificado expirou.

6.2.20.3. O titular dos dados pessoais revogou o consentimento.

6.2.20.4. A Autoridade Nacional de Proteção de Dados determinou.

6.2.21. A conservação dos dados pessoais está autorizada nas seguintes situações:

6.2.21.1. Para cumprimento de obrigação legal ou regulatória pelo controlador.

6.2.21.2. Para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

6.2.21.3. Para transferência a terceiro, desde que respeitados os requisitos de tratamento de dados da legislação nacional.

6.2.21.4. Para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

6.2.22. Quando atuar como Operador, a Vexia realizará o tratamento conforme as instruções do Controlador, garantindo uma finalidade específica e atendendo aos requisitos legais aplicáveis.

6.2.22.1. A responsabilidade pela determinação do embasamento legal válido para o tratamento dos dados pessoais caberá ao Controlador, podendo o Operador, recusar o tratamento caso identifique incoerência entre finalidade e tratamento dos dados pessoais.

6.2.23. A VEXIA, diante da necessidade de cumprimento de obrigações legais ou regulatórias, manutenção e execução de contratos, exercício regular de direitos em processo judicial, administrativo ou arbitral ou por meio do legítimo interesse, poderá compartilhar dados com outras empresas e até mesmo com a administração pública.

6.2.23.1. A VEXIA exige contratualmente que estes terceiros apresentem garantias técnicas e organizacionais apropriadas para proteger os dados pessoais, de forma que o tratamento satisfaça os requisitos da lei aplicável e assegure a segurança e a proteção dos direitos dos titulares dos dados.

6.2.23.2. Quando da transferência de dados pessoais, a empresa terceira deverá manter registros dos tratamentos realizados, bem como garantir a não alteração da finalidade inicialmente pretendida.

6.2.23.3. Poderão ocorrer inspeções regulares nas empresas receptoras dos dados pessoais. A VEXIA poderá avaliar as condições oferecidas para o tratamento de dados pessoais transferidos. Tais inspeções, caso ocorram, serão documentadas, a fim de, se necessário, serem apresentadas como evidências em questões futuras.

6.2.23.4. Caso sejam analisadas pequenas inconsistências, a VEXIA poderá fornecer prazo limite para a adequação das empresas terceiras aos requisitos legais e/ou exigências contratuais. Nessa situação a VEXIA assumirá eventuais riscos durante o período de adequação.

6.2.23.5. Caso seja detectado grande inconsistência, deverá ser estudado a possibilidade de encerramento imediato do contrato, evitando a incidência de riscos para os dados pessoais compartilhados.

6.2.23.6. Transferência de mídias digitais e físicas deverão ser realizadas mediante a utilização de meios de transporte seguros, garantidos contra extravios e acessos indevidos.

6.2.24. Para a transferência internacional de dados, a Vexia poderá coletar o consentimento do titular dos dados de forma específica e destacada, garantindo que ele seja informado previamente sobre o caráter internacional da operação e distinguindo claramente essa finalidade das demais.

6.2.25. Caso não seja aplicável o consentimento, a transferência internacional somente poderá ocorrer nos seguintes casos, bem como observada a Resolução CD/ANPD nº 19, de 23 de agosto de 2024:

6.2.25.1. Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais nos mesmos moldes da legislação nacional.

6.2.25.2. Quando o Controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados nos mesmos moldes da legislação nacional, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos;

6.2.25.3. Quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional.

6.2.25.4. Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros.

6.2.25.5. Quando a autoridade nacional autorizar a transferência.

6.2.25.6. Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional.

6.2.25.7. Quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público.

6.2.25.8. Para o cumprimento de obrigação legal ou regulatória pelo controlador.

6.2.25.9. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

6.2.25.10. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

6.2.26. A VEXIA criará e manterá um Comitê de Cyber e Proteção de Dados, formado por profissionais indicados pelas seguintes áreas da empresa: Auditoria e Riscos (Segurança da Informação), Diretoria, Compliance, Sistemas/Transformação Digital e Tecnologia da Informação e presidido pelo Encarregado pelo Tratamento de Dados Pessoais ou "DPO".

6.2.26.1. A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no website da VEXIA.

6.2.26.2. Em caso de DPO as a service (terceirizado), além da razão social da empresa contratada para este fim, deverá ser divulgado também o nome completo da pessoa natural que a representa nesta atividade, conforme Resolução CD/ANPD nº 18, de 16 de julho de 2024.

6.2.27. As atividades do Encarregado pelo Tratamento de Dados Pessoais consistem em:

6.2.27.1. Aceitar reclamações e comunicações dos titulares de dados pessoais, prestar esclarecimentos e adotar providências;

6.2.27.2. Receber comunicações da autoridade nacional e adotar as providências necessárias, demandando as áreas internas para o cumprimento;

6.2.27.3. Orientar, por meio do Comitê de Cyber e Proteção de Dados, os funcionários e os contratados da empresa sobre as práticas a serem tomadas em relação à proteção de dados pessoais; e

6.2.27.4. Quando necessário ou conforme disposição legal, solicitar ao departamento responsável a elaborações do Relatório de Impacto de Proteção de Dados e validar tal documento;

6.2.27.5. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;

6.2.27.6. Avaliar o registro de tratamento de dados sempre que ocorrer algum tipo de alteração no tratamento. Em caso de verificação de inconsistência na análise ou de risco no tratamento, poderá solicitar ao departamento responsável pelos dados a realização de um Relatório de Impacto de Proteção de Dados para o tratamento apontado.

6.2.27.7. Monitorar a conformidade da VEXIA com a LGPD e por qualquer outra legislação aplicável à proteção dos Dados Pessoais;

6.2.27.8. Validar os atos do Comitê de Cyber e Proteção de Dados;

6.2.27.9. Conduzir ações corretivas e preventivas em caso de detecção de alguma não conformidade;

6.2.27.10. Notificar a ANPD, sem demora injustificada e, quando possível, no prazo de 3 dias úteis, observando as diretrizes da norma de gestão de incidentes (023 - NOR - I - AR - Segurança da Informação - Gerenciamento de Incidentes e Vazamento de Dados), sobre as violações de dados pessoais que importem risco para os direitos e liberdades dos titulares dos dados.

6.2.28. O Comitê de Cyber e Proteção de Dados é responsável pela conformidade da Vexia à legislação e suas atividades consistem em:

6.2.28.1. Realizar encontros quinzenais, com a elaboração de atas;

6.2.28.2. Elaborar indicadores-chaves de sucesso para avaliar a implementação do programa de proteção de dados, buscando a excelência no tratamento lícito de dados;

6.2.28.3. Elaborar mecanismo de informação ao titular dos dados quando da coleta de tais informações.

6.2.28.4. Desenvolver e manter políticas, normas, procedimentos e padrões de conduta sobre a temática e garantir que os dados pessoais são recolhidos legalmente;

6.2.28.5. Realizar, anualmente, treinamento referente às questões de proteção de dados pessoais, com vista a assegurar o conhecimento por parte dos colaboradores acerca das obrigações que lhes são impostas neste âmbito;

6.2.28.6. Interagir com os departamentos internos para a resolução de questões legais e técnicas relacionadas a privacidade e proteção de dados;

6.2.28.7. Investigar e apurar possíveis violações de privacidade de dados, bem como formalizar e tomar as medidas corretivas adequadas em tempo hábil;

6.2.28.8. Garantir e prestar suporte ao Encarregado de Proteção de Dados para a elaboração dos comunicados aos titulares de dados e a Autoridade Nacional de Proteção de Dados;

6.2.28.9. Implementar diretrizes e desenvolver o Registro das operações de tratamento de dados pessoais;

6.2.28.10. Implementar diretrizes e desenvolver o Relatório de Impacto de Proteção de Dados pessoais;

6.2.28.11. Desenvolver e implementar mecanismo de acesso razoável para permitir que os titulares dos dados possam solicitar correção, eliminação ou transmissão dos seus dados pessoais, se apropriado ou exigido por lei, ou em casos de revogação do consentimento;

6.2.28.12. Manter o registro das solicitações para corrigir, alterar ou destruir os dados pessoais;

6.2.28.13. Implementar e garantir que as solicitações dos titulares de dados sejam cumpridas dentro de um prazo de 15 dias, como determina a lei. As demais solicitações serão atendidas em prazo razoável, até que ocorra determinação da Autoridade Nacional de Proteção de Dados (ANPD).

6.2.28.14. Garantir que os operadores ou outros controladores a quem os dados pessoais tenham sido transmitidos sejam informados, em data hábil, sobre as solicitações de apagamentos, retificações ou outras interações advindas dos direitos do próprio titular dos dados;

6.2.28.15. Assegurar o cumprimento dos processos conforme as disposições deste documento;

6.2.28.16. Implementar as melhorias conforme definido neste normativo;

6.2.28.17. Gerar, medir e analisar os dados relacionados a esse processo;

6.2.28.18. Fornecer informações necessárias para a análise crítica da gestão e implementar as ações acordadas;

6.2.28.19. Apurar violação de dados pessoais, suspeita ou real;

6.2.28.20. Atualizar a Política de Privacidade dos sites e aplicativos a qualquer tempo, sempre que uma alteração significativa ocorrer.

6.2.29. A Vexia garante aos titulares dos dados o exercício de direitos, mediante solicitação através do e-mail dpo@vexia.com.br, para:

6.2.29.1. Confirmação da existência de tratamento.

6.2.29.2. Acessar os dados.

6.2.29.3. Corrigir dados incompletos, inexatos ou desatualizados.

6.2.29.4. Anonimizar, bloquear ou eliminar de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.

6.2.29.5. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador.

6.2.29.6. Acessarem as informações sobre quais foram as entidades públicas e privadas com quem o controlador realizou uso compartilhado de dados.

6.2.29.7. Rever decisões automatizadas dos seus sistemas de inteligência artificial.

6.2.30. Mediante solicitação, os titulares dos dados têm o direito de obter da Vexia a eliminação dos seus dados pessoais, sendo permitida a manutenção dos dados pessoais em alguns casos conforme descrito no item 6.2.21. Quando a Vexia atuar como Controladora, o Comitê de Cyber e Proteção de Dados deve tomar as medidas necessárias (incluindo medidas técnicas) para informar os terceiros que usam ou processam esses dados para atender à solicitação.

6.2.31. Quando a Vexia verificar uma violação de dados pessoais, suspeita ou real, após apuração do Comitê de Cyber e Proteção de Dados, caso exista qualquer risco para os direitos e liberdades dos titulares dos dados, o Encarregado pelo Tratamento de Dados Pessoais deverá notificar a ANPD, sem demora injustificada e, quando possível, no prazo de 3 dias úteis, observando as diretrizes da norma de gestão de incidentes (023 - NOR - I - AR - Segurança da Informação - Gerenciamento de Incidentes e Vazamento de Dados).

6.2.32. A Vexia, através do seu Comitê de Cyber e Proteção de Dados e DPO, atualizará a Política de Privacidade dos sites e aplicativos a qualquer tempo, sempre que uma alteração significativa ocorrer, com a respectiva notificação das partes interessadas.

6.2.33. A Vexia reserva o direito de, a qualquer momento, atualizar ou modificar esta Norma e as políticas de privacidade, publicando uma versão atualizada nos seus respectivos portais e nos seus websites. Em caso de modificação dessa Norma ou qualquer política de privacidade, as modificações só se aplicarão às informações pessoais que forem coletadas após a publicação da versão revisada desta Norma ou da política de privacidade.

6.2.34. A Vexia considera o risco para os indivíduos cujos dados pessoais identificáveis são processados, realizando uma análise de risco criteriosa que suporta a tomada de decisões em sua matriz de riscos corporativa e o relatório de impacto de dados pessoais (RIPD).

7. MEDIDAS DISCIPLINARES

O descumprimento das diretrizes estipuladas nesta Norma caracteriza uma situação de não conformidade e para tanto, deverá ser apontada conforme procedimento específico. Tal fato será objeto de avaliação e poderá levar à aplicação de medidas administrativas, conforme determina a Política de Medidas Disciplinares da VEXIA.
Aquele que adotar ações de retaliação contra qualquer pessoa que tenha, em boa-fé, suscitado questões ou preocupações de conformidade com esta norma estará sujeito a sanções disciplinares.

8. CONFIDENCIALIDADE

Este documento é de propriedade da VEXIA, porém, em virtude de suas características, seu uso é **PÚBLICO**, podendo ser impresso e/ou divulgado sem necessidade de autorização expressa da área de Compliance.

9. APROVAÇÕES

Responsável pela Elaboração		
Nome Rodolfo Cesar Porte	Função Assistente Jurídico	Data 09/11/2020
Responsável pela Revisão		
Nome Cristiane Ziggiatti	Função Consultora	Data 14/07/2025

Responsável pela Aprovação		
Aprovação por sistema SIM (x) NÃO ( )	N° Documento INC6747539	
Nome Alvaro Villalobos	Área Responsável Compliance	Data 04/08/2025

10. HISTÓRICO DE REVISÕES

Revisão:	**Nº do Documento:**	**Data:**
03	INC6747539	10/07/2025
Itens revisados nesta versão Item 3 - Referências - referências externas e internas; Item 4 - Definições - ordenação alfabética e redação; Item 5 - Responsabilidades - ajustado para refletir o descrito na norma; Item 6 - Diretrizes Especificas - ajustado para melhor compreensão com referências normativas internas e as novas resoluções emitidas pela ANPD.		**Revisado por** Débora Ferraz
Histórico de Revisões: **Revisão 01 de 06/01/2023 - INC6309070** • Inclusão do nome da área no item de Confidencialidade. **Revisão 02 de 30/06/2023 - INC6400740** • base legal para o tratamento de dados de criança e adolescentes; • responsabilidades do comitê de proteção de dados; **Revisão 03 de 10/07/2025 - INC6747539** • Item 3 - Referências - referências externas e internas; • Item 4 - Definições - ordenação alfabética e redação;		

- Item 5 - Responsabilidades - ajustado para refletir o descrito na norma;
- Item 6 - Diretrizes Especificas - ajustado para melhor compreensão com referências normativas internas e as novas resoluções emitidas pela ANPD.
- Alteração da prática/ área responsável pela norma de Jurídico para Compliance.