POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS

TECPRO SERVICES LTDA

Código: PI-JUR – 03/26

Versão: 1.0

Data de Vigência: 08/06/2026

Área Proprietária: Diretoria Jurídica

Áreas Corresponsáveis: Departamento de Compliance, Presidência, Financeiro, Comercial, Operações e demais áreas técnicas demandantes.

Aprovação: Presidência e Comitê Executivo de Prevenção e Combate à Corrupção e Compliance.

POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

NOTA DE USO

Este documento corresponde a instituição de regulamento interno para orientar colaboradores, prestadores, fornecedores e parceiros sobre o tratamento de dados pessoais no âmbito da Tecpro. O texto deve ser adaptado aos processos reais da empresa, aos contratos vigentes, aos sistemas utilizados, ao inventário de dados e às decisões do Encarregado pelo Tratamento de Dados Pessoais.

O regulamento não substitui parecer jurídico específico em caso de dúvida, conflito normativo ou situação sensível, ocasião pelo qual a área responsável deve consultar o Encarregado/DPO e o Jurídico.

CAPÍTULO I - OBJETIVO

Este Regulamento estabelece diretrizes, regras e responsabilidades para o tratamento de dados pessoais realizado pela Tecpro, em conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD, com as regulamentações aplicáveis da Autoridade Nacional de Proteção de Dados - ANPD e com boas práticas de governança, segurança da informação, privacidade e proteção dos direitos dos titulares.

O objetivo é assegurar que as atividades da empresa sejam conduzidas de forma ética, transparente, segura e responsável, reduzindo riscos legais, regulatórios, reputacionais, comerciais e operacionais decorrentes do uso inadequado de dados pessoais.

CAPÍTULO II – ABRAGÊNCIA

Este Regulamento aplica-se a todos que atuem em nome da Tecpro ou tenham acesso a dados pessoais tratados pela empresa, incluindo:

- colaboradores, aprendizes, estagiários, sócios, administradores e gestores;

- prestadores de serviços, consultores, terceiros e profissionais alocados em projetos;
- fornecedores, parceiros comerciais, canais de venda, operadores de dados e subcontratados;
- áreas internas que realizem coleta, uso, armazenamento, compartilhamento, análise, exclusão, arquivamento ou qualquer outra operação com dados pessoais.

O Regulamento abrange dados pessoais de clientes, leads, prospects, colaboradores, candidatos a vagas, dependentes, visitantes, fornecedores, usuários de sites, parceiros e demais pessoas naturais relacionadas às atividades da empresa.

CAPÍTULO III - DEFINIÇÕES

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, e-mail, telefone, endereço, imagem, voz, cargo, dados profissionais, dados financeiros, identificadores digitais ou registros de acesso.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dado referente à saúde ou à vida sexual, dado genético ou biométrico vinculado a uma pessoa natural.

Titular: pessoa natural a quem se referem os dados pessoais tratados.

Tratamento: qualquer operação realizada com dados pessoais, incluindo coleta, acesso, armazenamento, uso, compartilhamento, transmissão, alteração, classificação, arquivamento, eliminação ou anonimização.

Controlador: pessoa física ou jurídica responsável pelas decisões referentes ao tratamento de dados pessoais.

Operador: pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado/DPO: pessoa indicada para atuar como canal de comunicação entre a empresa, os titulares dos dados e a ANPD, além de orientar colaboradores e apoiar a governança de privacidade.

Incidente de segurança: evento confirmado ou suspeito que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais.

Anonimização: uso de meios técnicos razoáveis para que um dado deixe de ser associado, direta ou indiretamente, a uma pessoa natural.

Eliminação: exclusão de dados pessoais ou descarte seguro de documentos físicos, observados os prazos legais e regulatórios aplicáveis.

CAPÍTULO IV – PRINCÍPIOS DE PROTEÇÃO DE DADOS

Todo tratamento de dados pessoais realizado pela Tecpro deverá observar os princípios previstos na LGPD, especialmente:

- Finalidade: tratamento para propósitos legítimos, específicos, explícitos e informados ao titular.
- Adequação: compatibilidade entre o tratamento e as finalidades informadas.
- Necessidade: limitação do tratamento ao mínimo necessário para a finalidade pretendida.
- Livre acesso: possibilidade de consulta facilitada e gratuita sobre a forma e duração do tratamento, quando aplicável.
- Qualidade dos dados: manutenção de dados exatos, claros, relevantes e atualizados.

- Transparência: fornecimento de informações claras, precisas e acessíveis aos titulares.
- Segurança: uso de medidas técnicas e administrativas para proteger os dados pessoais.
- Prevenção: adoção de medidas para evitar danos decorrentes do tratamento de dados pessoais.
- Não discriminação: vedação de tratamento para fins discriminatórios, ilícitos ou abusivos.
- Responsabilização e prestação de contas: demonstração de medidas eficazes de conformidade e governança.

CAPÍTULO V - BASES LEGAIS PARA TRATAMENTO

Todo tratamento de dados pessoais deverá estar vinculado a uma base legal válida. A área responsável pelo processo deve identificar e documentar a base legal aplicável antes da coleta ou uso dos dados.

- consentimento do titular, quando necessário e apropriado;
- cumprimento de obrigação legal ou regulatória;
- execução de contrato ou procedimentos preliminares relacionados a contrato;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- legítimo interesse, mediante avaliação de necessidade, proporcionalidade e expectativa do titular;
- proteção ao crédito;
- proteção da vida ou da incolumidade física;
- tutela da saúde, quando aplicável;
- outras hipóteses previstas na legislação aplicável.

O tratamento de dados pessoais sensíveis deverá observar hipóteses legais específicas, ser restrito ao necessário e contar com controles reforçados de acesso, segurança e confidencialidade.

CAPÍTULO VI - RESPONSABILIDADES

Diretoria

- aprovar e apoiar o Programa de Privacidade e Proteção de Dados;
- garantir recursos compatíveis com os riscos e obrigações da empresa;
- promover cultura de privacidade, ética e segurança da informação;
- avaliar riscos relevantes e apoiar decisões sobre incidentes, fornecedores críticos e projetos estratégicos.

Encarregado pelo Tratamento de Dados Pessoais – DPO

- atuar como canal de comunicação entre a empresa, os titulares dos dados e a ANPD;
- receber solicitações, reclamações e comunicações relacionadas a dados pessoais;
- orientar colaboradores, prestadores e áreas internas sobre práticas de proteção de dados;
- apoiar a avaliação de riscos, incidentes, fornecedores e novos projetos;
- manter registros, evidências e documentos relacionados ao programa de privacidade;
- recomendar melhorias em políticas, procedimentos, avisos de privacidade e contratos.

Gestores de Área

- assegurar que suas equipes tratem dados pessoais apenas quando necessário;
- mapear processos que envolvam dados pessoais e comunicar mudanças relevantes ao Encarregado/DPO;
- restringir acessos, revisar permissões e evitar compartilhamentos indevidos;
- acionar o Encarregado/DPO em novos projetos, campanhas, integrações, sistemas ou contratações que envolvam dados pessoais;
- garantir que fornecedores sob sua gestão cumpram obrigações de proteção de dados.

Colaboradores e Prestadores

- acessar apenas dados necessários às suas atividades profissionais;

- manter sigilo sobre dados pessoais e informações corporativas;
- não copiar, exportar, transferir ou compartilhar bases de dados sem autorização;
- não utilizar dados pessoais para fins particulares, discriminatórios ou incompatíveis com a finalidade autorizada;
- proteger credenciais, dispositivos, documentos físicos e arquivos digitais;
- comunicar imediatamente qualquer suspeita de incidente, vazamento ou uso indevido.

Tecnologia e Segurança da Informação

- implementar controles técnicos compatíveis com os riscos dos sistemas e processos;
- gerir acessos, autenticação, logs, backups, criptografia, monitoramento e resposta a incidentes, quando aplicável;
- apoiar a avaliação de fornecedores, integrações, ambientes em nuvem e sistemas corporativos;
- assegurar descarte seguro de equipamentos, mídias e documentos digitais;
- orientar a empresa sobre boas práticas de segurança da informação.

Recursos Humanos

O RH deverá tratar dados de colaboradores, candidatos e dependentes apenas para finalidades trabalhistas, previdenciárias, administrativas, contratuais, legais, de benefícios, saúde ocupacional, segurança e gestão de pessoas, observando necessidade, confidencialidade e retenção adequada.

Marketing e Comercial

As áreas de Marketing e Comercial deverão tratar dados de leads, prospects, clientes e contatos de relacionamento com transparência, base legal adequada, controle de origem dos dados, segmentação responsável e mecanismos de descadastramento ou oposição quando aplicáveis.

Coleta e Uso de Dados Pessoais

A coleta de dados pessoais deve ser limitada ao necessário para a finalidade pretendida. Antes de iniciar uma nova coleta, formulário, campanha, sistema, integração, automação ou projeto que envolva dados pessoais, a área responsável deverá avaliar:

- quais dados serão coletados e por qual motivo;
- qual é a finalidade do tratamento;
- qual base legal será utilizada;
- quem terá acesso aos dados;
- por quanto tempo os dados serão armazenados;
- se haverá compartilhamento com terceiros ou transferência internacional;
- quais riscos podem afetar os titulares;
- se será necessário aviso de privacidade, consentimento, relatório de impacto ou revisão contratual.

É proibida a coleta excessiva, desnecessária, oculta ou incompatível com a finalidade informada ao titular ou aprovada internamente.

Compartilhamento de Dados com Terceiros

O compartilhamento de dados pessoais com terceiros somente poderá ocorrer quando houver finalidade legítima, base legal adequada, necessidade operacional, autorização interna e medidas contratuais e de segurança compatíveis.

Contratos com fornecedores, operadores, parceiros e subcontratados que tratem dados pessoais devem conter cláusulas de proteção de dados, incluindo, quando aplicável:

- finalidade e limites do tratamento;
- obrigações de confidencialidade;

- medidas técnicas e administrativas de segurança;
- restrição de uso dos dados para fins próprios ou incompatíveis;
- regras para subcontratação;
- prazos e forma de comunicação de incidentes;
- devolução, eliminação ou anonimização dos dados ao fim da relação;
- cooperação no atendimento de solicitações de titulares, auditorias e autoridades.

CAPÍTULO IX – TRANSFERÊNCIA INTERNACIONAL DE DADOS

Caso a Tecpro utilize sistemas, ferramentas, plataformas de nuvem, fornecedores ou suboperadores que armazenem, processem ou acessem dados pessoais fora do Brasil, a transferência internacional deverá observar as hipóteses legais e regulamentares aplicáveis, incluindo garantias contratuais, controles de segurança e avaliação do país, organismo ou mecanismo de transferência utilizado.

A área responsável deve consultar o Encarregado/DPO antes de contratar ou alterar ferramenta que envolva transferência internacional de dados pessoais.

CAPÍTULO X – DIREITOS DOS TITULARES

A Tecpro deverá assegurar aos titulares o exercício dos direitos previstos na LGPD, incluindo, quando aplicável:

- confirmação da existência de tratamento;
- acesso aos dados pessoais;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade;
- portabilidade dos dados, quando regulamentada e aplicável;
- informação sobre entidades públicas e privadas com as quais houve compartilhamento;

- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- revogação do consentimento;
- oposição ao tratamento em caso de descumprimento da LGPD;
- revisão de decisões tomadas unicamente com base em tratamento automatizado, quando aplicável.

Os pedidos deverão ser enviados pelo canal oficial de privacidade: [inserir e-mail ou formulário LGPD]. A empresa poderá solicitar informações adicionais para confirmar a identidade do titular e proteger os dados contra acesso indevido.

O atendimento poderá ser limitado, negado ou justificado quando houver obrigação legal, segredo comercial, prevenção à fraude, exercício regular de direitos, proteção de terceiros ou outra hipótese legítima prevista na legislação.

CAPÍTULO XI – SEGURANÇA DA INFORMAÇÃO

A Tecpro adotará medidas técnicas e administrativas para proteger dados pessoais contra acessos não autorizados, perda, destruição, alteração, comunicação indevida ou qualquer forma de tratamento inadequado ou ilícito.

São regras obrigatórias para todos os colaboradores, prestadores e terceiros:

- não compartilhar senhas, tokens, códigos de autenticação ou acessos corporativos;
- utilizar autenticação multifator sempre que disponível ou exigida;
- bloquear a tela ao se ausentar do computador;
- armazenar arquivos corporativos apenas em ambientes autorizados pela empresa;
- não enviar dados pessoais por canais informais ou não autorizados;
- não baixar bases de dados em dispositivos pessoais;
- não utilizar e-mails pessoais para atividades corporativas;

- manter documentos físicos em locais seguros e com acesso restrito;
- descartar documentos com dados pessoais por meio seguro, como fragmentação ou coleta autorizada;
- comunicar imediatamente qualquer suspeita de incidente ou acesso indevido.

CAPÍTULO XII – RETENÇÃO E ELIMINAÇÃO DE DADOS

Dados pessoais deverão ser mantidos apenas pelo tempo necessário ao cumprimento da finalidade, de obrigação legal ou regulatória, de obrigação contratual, de exercício regular de direitos ou de outra hipótese legítima.

Ao final do prazo aplicável, os dados deverão ser eliminados, anonimizados ou arquivados de forma segura, conforme tabela de temporalidade interna, quando existente.

A eliminação deverá observar requisitos legais, fiscais, trabalhistas, contábeis, regulatórios, contratuais, técnicos e de defesa judicial.

CAPÍTULO XIII – DADOS PESSOAIS SENSÍVEIS

O tratamento de dados pessoais sensíveis deve ser excepcional, restrito ao necessário, documentado e protegido por controles reforçados.

- O acesso deve ser limitado a pessoas autorizadas e com necessidade funcional.
- A coleta deve ser precedida de análise da finalidade e da base legal aplicável.
- Dados de saúde, biometria, atestados, informações sindicais ou dados de dependentes devem receber proteção adicional.
- É proibido tratar dados sensíveis para fins discriminatórios, abusivos ou incompatíveis com a finalidade autorizada.

CAPÍTULO XIV – DADOS DE CRIANÇAS E ADOLESCENTES

O tratamento de dados pessoais de crianças e adolescentes deverá observar o melhor interesse do menor, ser limitado ao necessário e ocorrer conforme as hipóteses legais aplicáveis.

Quando necessário, deverá haver consentimento específico e em destaque por pelo menos um dos pais ou responsável legal, salvo hipóteses legais que dispensem o consentimento.

CAPÍTULO XV – MARKETING, COMUNICAÇÃO E USO DE IMAGEM

A utilização de dados pessoais para campanhas, eventos, newsletters, materiais institucionais, relacionamento comercial, prospecção, CRM, automação de marketing e mídia paga deverá respeitar finalidade, base legal, transparência e mecanismos de oposição ou descadastramento, quando aplicáveis.

- Listas de contatos não poderão ser compradas, compartilhadas ou utilizadas sem validação de origem, finalidade e base legal.
- O uso de imagem, voz, depoimentos ou identificação de colaboradores, clientes e parceiros em materiais institucionais deverá observar autorização adequada, quando necessária.
- Campanhas segmentadas devem evitar critérios discriminatórios, sensíveis ou incompatíveis com a expectativa razoável dos titulares.
- Comunicações comerciais devem respeitar preferências de opt-out, descadastramento e oposição.

CAPÍTULO XVI – COOKIES E TECNOLOGIAS DE RASTREAMENTO

Sites, landing pages e plataformas digitais da Tecpro deverão informar, de forma clara, o uso de cookies e tecnologias similares.

- Cookies necessários poderão ser utilizados para funcionamento do ambiente digital.

- Cookies analíticos, publicitários ou de personalização devem observar transparência, gestão de preferências e base legal adequada.
- Ferramentas de medição, pixels, tags e integrações com mídia paga devem ser avaliadas pela área responsável, pelo Encarregado/DPO e por Segurança da Informação quando houver risco relevante.

CAPÍTULO XVII – INCIDENTES DE SEGURANÇA

Qualquer colaborador, prestador ou terceiro que identificar ou suspeitar de incidente envolvendo dados pessoais deverá comunicar imediatamente o Encarregado/DPO e a área de Segurança da Informação pelo canal: [inserir canal interno de incidente].

Exemplos de incidentes:

- envio de e-mail com dados pessoais para destinatário errado;
- perda, furto ou roubo de notebook, celular, mídia ou documento físico;
- acesso indevido a sistema ou base de dados;
- vazamento, exposição pública ou publicação indevida de informações;
- ransomware, malware, phishing ou comprometimento de credenciais;
- exclusão, alteração ou compartilhamento indevido de dados pessoais.

A empresa deverá registrar, investigar, classificar e tratar incidentes de segurança. Quando o incidente puder ocasionar risco ou dano relevante aos titulares, o controlador deverá avaliar comunicação à ANPD e aos titulares, conforme regulamentação aplicável.

CAPÍTULO XVIII – PRIVACIDADE DESDE A CONCEPÇÃO

Novos projetos, produtos, sistemas, integrações, campanhas, automações, processos ou contratações que envolvam dados pessoais deverão considerar proteção de dados desde a concepção e por padrão.

A área responsável deverá consultar o Encarregado/DPO quando houver:

- tratamento de grande volume de dados pessoais;
- uso de dados sensíveis;
- monitoramento sistemático de pessoas;
- decisões automatizadas com impacto relevante;
- compartilhamento com terceiros ou transferência internacional;
- nova tecnologia, integração ou fornecedor crítico;
- risco elevado aos direitos e liberdades dos titulares.

CAPÍTULO XIX – RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Quando aplicável, a empresa poderá elaborar Relatório de Impacto à Proteção de Dados Pessoais - RIPD, contendo descrição dos processos de tratamento, fundamentos, riscos aos titulares e medidas de mitigação.

A necessidade de RIPD deverá ser avaliada pelo Encarregado/DPO em conjunto com a área responsável, Jurídico, Segurança da Informação e Diretoria, conforme criticidade do tratamento.

CAPÍTULO XX – TREINAMENTO E CONSCIENTIZAÇÃO

A Tecpro Services Ltda (“Tecpro”) deverá promover treinamentos periódicos sobre privacidade, LGPD, segurança da informação e boas práticas no tratamento de dados pessoais.

- A participação poderá ser obrigatória para colaboradores e terceiros que tratem dados pessoais.
- Gestores devem incentivar a adesão aos treinamentos e reforçar boas práticas em suas equipes.
- Novos colaboradores devem receber orientação básica sobre este Regulamento durante o processo de integração.

CAPÍTULO XXI – AUDITORIA E MONITORAMENTO

A empresa poderá realizar auditorias, revisões, testes, verificações e monitoramentos internos para avaliar o cumprimento deste Regulamento, das políticas corporativas e da legislação aplicável.

As áreas deverão cooperar com solicitações do Encarregado/DPO, Jurídico, Compliance, Segurança da Informação, Auditoria ou Diretoria.

CAPÍTULO XXII – MEDIDAS DISCIPLINARES

O descumprimento deste Regulamento poderá resultar em medidas disciplinares, conforme gravidade, reincidência e impacto do ato, incluindo advertência, suspensão, desligamento, rescisão contratual, bloqueio de acessos, responsabilização civil ou comunicação às autoridades competentes.

O uso indevido de dados pessoais para benefício próprio, divulgação não autorizada, cópia irregular de bases, vazamento intencional ou omissão de incidente poderá ser considerado falta grave.

CAPÍTULO XXIII – CONTRATAÇÃO DE FORNECEDORES

Antes da contratação de fornecedores que tratem dados pessoais, a área responsável deverá avaliar, conforme criticidade:

- finalidade do tratamento e categorias de dados envolvidos;
- reputação e maturidade de segurança do fornecedor;
- localização do armazenamento e eventual transferência internacional;
- medidas de segurança, controles de acesso, logs e backups;
- suboperadores e subcontratados envolvidos;
- histórico de incidentes ou fragilidades conhecidas;
- contrato com cláusulas de proteção de dados;
- canal e prazo para comunicação de incidentes;
- possibilidade de auditoria, evidências de conformidade ou certificações.

CAPÍTULO XXIV – REGISTRO DE OPERAÇÕES DE TRATAMENTO

A Tecpro deverá manter registro das principais operações de tratamento de dados pessoais, contendo, quando aplicável:

- área responsável e dono do processo;
- finalidade do tratamento;
- categorias de dados pessoais e de titulares;
- base legal utilizada;
- sistemas, planilhas, repositórios e ferramentas envolvidos;
- compartilhamentos com terceiros;
- transferência internacional, quando houver;
- prazos de retenção e descarte;
- medidas de segurança aplicáveis;
- fornecedores ou operadores envolvidos;
- avaliação de risco e necessidade de RIPD.

CAPÍTULO XXV – VIGÊNCIA E REVISÃO

Este Regulamento entra em vigor na data de sua aprovação e deverá ser revisado periodicamente, no mínimo a cada 12 meses, ou sempre que houver alteração legal, regulatória, operacional, tecnológica ou organizacional relevante.

A revisão será coordenada pelo Encarregado/DPO, com apoio das áreas de Jurídico, Segurança da Informação, Recursos Humanos, Marketing, Comercial, Operações e Diretoria, conforme aplicável.

CAPÍTULO XXVI – DISPOSIÇÕES GERAIS

Todos os colaboradores, prestadores e terceiros abrangidos por este Regulamento deverão ler, compreender e cumprir suas disposições.

Dúvidas sobre interpretação, aplicação ou exceções deverão ser encaminhadas ao Encarregado pelo Tratamento de Dados Pessoais pelo canal: [inserir canal LGPD].

CAPÍTULO XXVII – FONTES LEGAIS E NORMATIVAS DE REFERÊNCIA

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
- Autoridade Nacional de Proteção de Dados - ANPD: página de regulamentações vigentes. https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd
- Resolução CD/ANPD nº 18/2024 - Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. https://www.in.gov.br/
- Resolução CD/ANPD nº 15/2024 - Regulamento de Comunicação de Incidente de Segurança. https://www.in.gov.br/

• Resolução CD/ANPD nº 19/2024 - Regulamento de Transferência Internacional de Dados e cláusulas-padrão contratuais. https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd

ANEXO I - TERMO DE CIÊNCIA E COMPROMISSO

Declaro que recebi, li e compreendi o Regulamento Interno de Privacidade e Proteção de Dados Pessoais da Tecpro, comprometendo-me a cumprir suas disposições e a tratar dados pessoais de forma ética, segura, confidencial e em conformidade com a LGPD, políticas internas e orientações da empresa.

Também declaro estar ciente de que o descumprimento das regras poderá resultar em medidas disciplinares, contratuais, administrativas ou judiciais, conforme a gravidade da conduta e a legislação aplicável.

Nome completo: _____

CPF: _____

Cargo/Função: _____

Área _____

Data _____/_____/_____

Assinatura _____

ANEXO II - CHECKLIST RÁPIDO PARA ÁREAS INTERNAS

Antes de iniciar um novo processo, campanha, contratação, formulário, automação ou sistema que envolva dados pessoais, valide os itens abaixo:

Item Verificação Status/Observação

1 A finalidade do tratamento está clara e documentada. [ ] Conforme [ ] Ajustar

2 A base legal foi definida. [ ] Conforme [ ] Ajustar

3 A coleta está limitada ao mínimo necessário. [ ] Conforme [ ] Ajustar

4 O titular recebeu informação adequada, quando aplicável. [ ] Conforme [ ] Ajustar

5 O acesso aos dados será restrito a pessoas autorizadas. [ ] Conforme [ ] Ajustar

6 Há contrato ou cláusula de proteção de dados com fornecedores envolvidos.

[ ] Conforme [ ] Ajustar

7 Foi avaliada eventual transferência internacional. [ ] Conforme [ ] Ajustar

8 Há prazo de retenção ou critério de eliminação definido. [ ] Conforme [ ] Ajustar

9 Há medidas de segurança compatíveis com o risco. [ ] Conforme [ ] Ajustar

10 O Encarregado/DPO foi consultado em caso de dúvida ou risco relevante.

[ ] Conforme [ ] Ajustar