



Documento	OT – 004 - Política de Privacidade de Dados	
Classificação	Interno	
Referência Normativa: ISO 27001 e ISO 27701	Versão: 08	
Autor: Gerente de Segurança da Informação	Aprovação: Diretoria de Segurança da Informação	Efetivada em: 02/07/2026

1. Objetivo

Esta Política tem por objetivo estabelecer as diretrizes para o tratamento de dados pessoais realizado pela Ótima, assegurando a proteção dos direitos dos titulares, a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), as regulamentações da Autoridade Nacional de Proteção de Dados (ANPD) e a integração da privacidade ao Sistema de Gestão de Segurança da Informação (SGSI).

Esta Política também estabelece as diretrizes de governança em privacidade e proteção de dados pessoais, observando a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), as regulamentações expedidas pela Autoridade Nacional de Proteção de Dados (ANPD), bem como as melhores práticas nacionais e internacionais de segurança da informação e governança em privacidade.

2. Abrangência

Esta Política é aplicável a todas as empresas que integram a Ótima. O termo GRUPO ÓTIMA ou ÓTIMA refere-se ao Núcleo Empresarial que concentra as empresas que o integram expressamente. Portanto, este regramento se aplica a todas estas empresas e deve ser observado por empregados, prestadores de serviço, parceiros, enfim, a todos que tenham acesso a dados pessoais detidos pela Empresa ou em seu nome. Procedimentos adicionais podem ser criados de acordo com exigência da legislação vigente no País. A Legislação Vigente deve prevalecer caso esteja ou venha estar em conflito com esta Política em qualquer ponto.

Esta Política deverá ser interpretada em conjunto com as demais políticas corporativas, normas internas, contratos, procedimentos operacionais e controles do Sistema de Gestão de Segurança da Informação (SGSI).

2.1 Relação com o Contexto do SGSI

Esta Política integra o conjunto normativo de Segurança da Informação, Gestão de Riscos, Continuidade de Negócios, Gestão de Incidentes, Classificação da Informação, Controle de Acessos e demais políticas corporativas da organização.

3. Referências

Código de Conduta e Ética da Ótima

Política de Segurança da Informação

Lei Geral de Proteção de Dados Pessoais (“LGPD”)

Constituição da República Federativa do Brasil de 1988– Art. 5ª, X (“CRFB”);

Lei 8078/90 – Código de Defesa do Consumidor (“CDC”)

Lei 12.965/14 e seu Decreto Regulamentador 8771/18 – (“Marco Civil da Internet”)

ISO/IEC 27001:2022

ISO/IEC 27701:2019

Resolução CD/ANPD nº 19/2024 (Transferência Internacional de Dados)

Guia Orientativo da ANPD sobre Segurança da Informação

Guia da ANPD sobre Agentes de Tratamento e Encarregado

4. Definições

Accountability: princípio que estabelece a responsabilidade da organização em demonstrar a conformidade do tratamento de dados pessoais com a LGPD, por meio de controles, registros e evidências.

Confidencialidade: a confidencialidade está relacionada a privacidade dos dados.

Seu objetivo é restringir o acesso às informações, garantindo que ela chegue apenas às pessoas autorizadas.

Consentimento: consiste na manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais (“controlador”), sozinho ou juntamente a outros controladores (“co- controladores”).

Dados pessoais: são todas as informações que permitem a sua identificação. Como por exemplo, seu nome, cpf, e-mail, telefone, entre outros.

Dados pessoais sensíveis: são dados pessoais relacionados à 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 vinculados à pessoa física.

Disponibilidade: a disponibilidade é a garantia plena que a informação estará acessível sempre que seja necessário o seu uso.

DPO: encarregado de proteção de dados ou data protection officer (dpo) é a pessoa natural encarregada de supervisionar e dar suporte ao controlador ou ao operador em todos os temas relacionados ao tratamento de dados pessoais. O dpo desempenha um papel consultivo, ele/ela supervisiona a conformidade à LGPD, pelo controlador e o operador, e é a referência e ponto de contato com a autoridade nacional e com os titulares, de acordo com o que está previsto na LGPD e nesta política.

DPIA (Data Protection Impact Assessment): documento que identifica, avalia e registra os riscos do tratamento de dados pessoais, bem como as medidas adotadas para mitigá-los.

Incidente de segurança: qualquer evento que comprometa um dos pilares de segurança da informação, sendo eles confidencialidade, integridade e disponibilidade, exemplos: perda de informação, website indisponível ou acesso não autorizado a informações não públicas.

Integridade: a integridade consiste na veracidade e confiabilidade da informação, garantindo à preservação desta, garantindo sua manutenção conforme fora criada ou alterada mediante autorização.

Legítimo interesse: refere-se a uma das hipóteses autorizadoras para tratar dados pessoais (“bases legais”). A rigor, deve ser utilizado de maneira subsidiária às demais bases legais específicas e surge para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Operador: se trata de pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Salvo previsão expressa em sentido contrário, a ótima atuará na condição de operador de dados.

Privacy by Default: princípio que determina que produtos, serviços e sistemas adotem, por padrão, configurações que garantam o tratamento apenas dos dados pessoais estritamente necessários para cada finalidade.

Privacy by Design: princípio que determina que a proteção de dados pessoais seja considerada desde a concepção de produtos, serviços, sistemas e processos.

ROPA (Record of Processing Activities): registro das atividades de tratamento de dados pessoais realizadas pela organização, contendo informações necessárias para demonstrar conformidade com a LGPD.

Titular: se refere à pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência internacional de dados: será a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento de dados pessoais: significa qualquer operação, como 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, realizada com dados pessoais.

Violação de dados: é uma violação de segurança que leva ao acesso, divulgação não autorizada, alteração, perda ou destruição acidental ou ilegal de dados pessoais transmitidos, armazenados ou de outra forma tratados.

5. Da Coleta

A coleta de dados pessoais será realizada exclusivamente para finalidades legítimas, específicas e compatíveis com as atividades da organização, observando os princípios da finalidade, necessidade, adequação, transparência, minimização dos dados e as bases legais previstas na LGPD.

6. Do Uso das Informações

Toda atividade de tratamento de dados pessoais realizada pela Ótima será previamente avaliada quanto à sua finalidade e à respectiva base legal que a fundamenta, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). A identificação da base legal constitui requisito obrigatório para o tratamento dos dados pessoais e deverá ser compatível com a finalidade específica, observando os princípios da finalidade, adequação, necessidade, transparência, responsabilização e prestação de contas (accountability).

O tratamento de dados pessoais será realizado exclusivamente para finalidades legítimas, específicas, explícitas e compatíveis com as atividades desempenhadas pela organização, observando sempre os princípios da finalidade, adequação, necessidade, transparência, minimização dos dados, segurança e prevenção.

6.1 Bases legais aplicáveis

Conforme a natureza de cada operação de tratamento, poderão ser utilizadas, entre outras, as seguintes bases legais previstas na LGPD:

- ✓ Execução de contrato ou de procedimentos preliminares relacionados ao contrato;
- ✓ Cumprimento de obrigação legal ou regulatória;
- ✓ Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- ✓ Legítimo interesse do controlador ou de terceiros, quando aplicável e precedido da avaliação dos impactos aos direitos e liberdades dos titulares;
- ✓ Proteção da vida ou da incolumidade física do titular ou de terceiros;
- ✓ Consentimento do titular, quando exigido pela legislação;
- ✓ Demais hipóteses autorizadas previstas na Lei Geral de Proteção de Dados Pessoais.

6.2 Finalidades do tratamento

Os dados pessoais poderão ser tratados, conforme a natureza da relação existente entre a Ótima e o titular dos dados, para as seguintes finalidades:

- ✓ Executar contratos celebrados com clientes, parceiros, fornecedores e colaboradores, bem como realizar procedimentos preliminares relacionados à contratação;
- ✓ Cumprir obrigações legais, regulatórias ou determinações de autoridades competentes;
- ✓ Atender interesses legítimos da organização ou de terceiros, desde que observados os direitos e liberdades fundamentais dos titulares;
- ✓ Manter registros funcionais, cadastrais e de contato atualizados, inclusive para situações emergenciais;
- ✓ Gerenciar processos relacionados à administração de pessoal, incluindo recrutamento, desenvolvimento, desempenho, benefícios, remuneração e sucessão;
- ✓ Administrar registros de afastamentos, licenças legais e demais ocorrências relacionadas à gestão de pessoas;
- ✓ Cumprir obrigações relacionadas à saúde e segurança do trabalho, medicina ocupacional e acessibilidade;
- ✓ Assegurar a adequada administração das atividades corporativas e operacionais da organização;
- ✓ Atender solicitações de referências profissionais de colaboradores atuais ou antigos, quando autorizadas ou legalmente permitidas;
- ✓ Exercer, resguardar ou defender direitos em processos judiciais, administrativos ou arbitrais;

- ✓ Promover ações relacionadas à diversidade, igualdade de oportunidades e prevenção à discriminação no ambiente de trabalho.

Caso seja necessário tratar dados pessoais para finalidade diversa daquelas inicialmente informadas, a Ótima realizará previamente a avaliação da compatibilidade da nova finalidade com a base legal aplicável e, quando exigido pela legislação, fornecerá ao titular as informações pertinentes ou obterá seu consentimento.

A Ótima mantém o compromisso permanente de proteger os dados pessoais por meio da aplicação de controles técnicos e administrativos compatíveis com os riscos identificados, observando as diretrizes estabelecidas em sua Política de Segurança da Informação, Política de Segurança Cibernética, Código de Conduta e Ética e demais normas internas aplicáveis.

7. Registros dos Tratamentos de Dados Pessoais

A LGPD prevê que o Controlador e o Operador devem manter registro das operações de Tratamento que realizarem ("Registro") de forma independente um do outro. Para garantir o cumprimento da obrigação da LGPD, é primordial que haja um mapeamento dinâmico do Tratamento e seu ciclo de vida.

O conteúdo mínimo do Registro das Operações de Tratamento compreende:

- ✓ O nome e os dados de contato do Controlador e, quando aplicável, dos Controladores Conjuntos, do representante legal do Controlador e do Encarregado.
- ✓ As finalidades do Tratamento.
- ✓ Descrição das categorias de titulares e das categorias de Dados Pessoais.
- ✓ As categorias de destinatários para os quais os Dados Pessoais foram ou serão divulgados, incluindo destinatários em terceiros países ou organizações internacionais.
- ✓ Quando aplicável, as transferências internacionais de Dados Pessoais para outro país ou uma organização internacional, incluindo a identificação desse outro país ou organização internacional.
- ✓ O descarte de dados pessoais ocorrerá de acordo com os critérios estabelecidos na contratação dos serviços, obedecendo a legislação vigente e as normas de órgão regulador. A Ótima, em seus serviços atua como operadora de dados pessoais.
- ✓ Sempre que possível, uma descrição geral das medidas de segurança referidas no Art. 46 da LGPD.

Os registros das operações de tratamento constituem instrumento permanente de governança, responsabilização (accountability), transparência e melhoria contínua, permitindo adequada gestão dos riscos relacionados à privacidade.

7.1 Classificação e retenção de dados pessoais

Os dados pessoais e informações da Ótima são classificados conforme seu nível de sensibilidade e criticidade (ex.: público, interno, confidencial, restrito).

A retenção de dados pessoais segue critérios definidos com base nas obrigações legais e regulatórias, finalidade do tratamento e necessidade operacional. Cada nível de classificação possui requisitos específicos de controle de acesso, armazenamento, transmissão e descarte, definidos em normas internas complementares conforme política de classificação de dados da Ótima.

Após o término do prazo de retenção, os dados serão eliminados de forma segura ou anonimizados obedecendo os critérios de retenção.

8. Relatório de Impacto ("DPIA")

Sempre que identificado tratamento capaz de gerar riscos relevantes aos direitos e liberdades dos titulares, será avaliada a necessidade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais (DPIA), considerando critérios técnicos, jurídicos e operacionais.

O Relatório de Impacto à Proteção de Dados Pessoais é a documentação do Controlador que contém a descrição dos processos de Tratamento de Dados Pessoais que podem gerar riscos às liberdades

e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A Ótima, na condição de operadora, não é responsável pela elaboração do DPIA, sendo essa uma atribuição do Controlador. No entanto, deverá apoiar o Controlador sempre que necessário, fornecendo informações técnicas e operacionais para sua elaboração. Esclarecemos que o DPIA é um processo destinado a:

- ✓ Descrever o projeto ou o processo de Tratamento de dados e sua finalidade.
- ✓ Avaliar a necessidade e proporcionalidade do Tratamento.
- ✓ Avaliar os riscos dos direitos e liberdades do Titular decorrentes do Tratamento.
- ✓ Determinar as medidas de mitigação, e quando considerado necessário, o DPO deverá apresentar os resultados do DPIA à ANPD.
- ✓ O risco deve ser entendido como um risco de impacto negativo nos direitos e liberdades do Titular.
- ✓ A probabilidade e a gravidade do risco para os direitos e liberdades do Titular devem ser determinadas por referência à natureza, âmbito, contexto e finalidades do Tratamento. O risco deve ser avaliado com base em uma avaliação objetiva, através da qual se estabeleçam se as operações de Tratamento de dados envolvem um risco ou um alto risco.
- ✓ A LGPD não estabelece hipóteses nas quais a elaboração do DPIA é obrigatória, definindo apenas que a ANPD pode determinar sua execução. Dispõe, no entanto, em seu Art. 37 que o Controlador e o Operador devem manter registro das operações de Tratamento que realizarem, especialmente quando baseadas no Legítimo Interesse. Assim, o Controlador e o Operador deverão registrar o Tratamento de forma que seja viável a elaboração do DPIA em todas as situações em que haja Tratamento.

Sempre que aplicável, a Ótima colaborará com o Controlador para garantir a adequada avaliação de riscos aos direitos e liberdades dos titulares.

8.1 Gestão de Riscos de Segurança da Informação e Privacidade

A Ótima adota uma metodologia formal de gestão de riscos, que contempla:

- ✓ Identificação, análise e avaliação de riscos relacionados à segurança da informação e proteção de dados pessoais
- ✓ Definição de critérios de aceitação de risco
- ✓ Implementação de controles para mitigação
- ✓ Monitoramento contínuo e revisão periódica dos riscos

Os riscos são avaliados considerando impacto e probabilidade, e tratados conforme diretrizes do nosso sistema de gestão de segurança da informação. Os critérios de aceitação de risco são definidos pela organização e revisados periodicamente pela alta direção conforme política de gestão de riscos da Ótima.

9. Encarregado de Proteger os Dados (DATA PROTECTION OFFICER)

A LGPD exige que as organizações que realizam o Tratamento de Dados Pessoais nomeiem um Encarregado pelo Tratamento de Dados Pessoais (“DPO”) com o dever de exercer as atividades previstas no § 2º do Art. 41 da lei.

O DPO é selecionado considerando sua experiência em privacidade e proteção de dados, suas características profissionais, sua habilidade para cumprir as tarefas que lhe sejam atribuídas. O DPO pode ser um funcionário da Ótima ou um terceiro contratado para este serviço.

O Controlador e o Operador asseguram o envolvimento do DPO em todas as questões relativas à proteção de dados pessoais, garantindo sua independência na execução de suas funções:

- ✓ Garantidos os recursos necessários para executar seus deveres.
- ✓ Assegurando que ele/ela não receba instruções, nem seja penalizado por suas decisões e por seus pareceres.

- ✓ Garantindo que o DPO não atue em situações de conflitos de interesse.
- ✓ O DPO deve manter sua atividade em sigilo e confidencialidade, sendo responsável por garantir que haja o devido atendimento às reclamações e comunicações dos titulares, que sejam prestados os esclarecimentos e adotadas as providências necessárias. Apoiar e aconselhar o Controlador e o Operador em relação às obrigações decorrentes da legislação e regulamentação de proteção de dados, especialmente em relação à LGPD e às normas editadas pela ANPD.
- ✓ Projetar programas de conformidade e monitorar a implementação, definir governança de proteção de dados, avisos de privacidade padrão, cláusulas contratuais e boas práticas.
- ✓ Apoiar o Controlador e o Operador na negociação de contratos de proteção de dados, definir o fluxo de atendimento dos direitos dos titulares e definir e implementar planos de treinamento e conscientização regulares aos colaboradores, pois a cultura em segurança da informação e privacidade de dados é fundamental.
- ✓ Fornece, se necessário, uma opinião sobre a avaliação do impacto na proteção de dados e monitoramento de progresso.
- ✓ Cooperar e atuar como ponto de referência da ANPD, recebendo comunicações e adotando providências.
- ✓ Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.
- ✓ Orientar os funcionários e os contratados da Ótima a respeito das práticas a serem tomadas em relação à proteção de Dados Pessoais.

9.1 Conscientização

A Ótima mantém um programa contínuo de treinamento e conscientização em segurança da informação e privacidade de dados pessoais, para todos os seus colaboradores, que inclui:

- ✓ Treinamentos obrigatórios periódicos
- ✓ Campanhas de conscientização
- ✓ Avaliação de eficácia dos treinamentos

Os treinamentos são realizados mensalmente, além das campanhas de compliance que ocorrem quinzenalmente ou sempre que houver mudanças relevantes nos processos ou requisitos legais.

10. Definições quanto ao Controlador e Operador dos Dados

As atividades de tratamento serão conduzidas considerando não apenas a base legal aplicável, mas também a expectativa razoável do titular em relação ao uso de seus dados pessoais.

10.1 Controlador

Quando estiver atuando como Controlador, o que se dará excepcionalmente e se previsto expressamente, a Ótima observa as instruções emitidas pela ANPD e as diretrizes e práticas reconhecidas em matéria de proteção de Dados Pessoais.

O Controlador define a finalidade do Tratamento de Dados Pessoais e estabelece medidas técnicas e organizacionais apropriadas para assegurar a proteção de Dados Pessoais de acordo com a LGPD. Neste caso, a Ótima terá ainda o ônus de provar a conformidade com a LGPD e, com o suporte do DPO, tem o dever de:

- ✓ Planejar e executar as medidas adequadas de segurança, Privacy by design e Privacy by default, aplicando as melhores práticas e os mais altos padrões de mercado.
- ✓ Treinamento contínuo aos seus próprios empregados e terceiros.
- ✓ Verificar o cumprimento da LGPD nos terceiros que tratam os dados em seu nome, quando assim ocorrer, no entanto, em nossos serviços e plataformas a Ótima não terceiriza suas operações.
- ✓ Cooperar com a ANPD nos cursos de suas iniciativas de investigação.
- ✓ Os Controladores, quando conjuntos, estabelecem de forma transparente, mediante acordo, suas respectivas responsabilidades em relação ao cumprimento das obrigações decorrentes da LGPD, em especial no que diz respeito ao exercício dos direitos pelos titulares.

10.2 Operador

A Ótima quando estiver atuando como Operador, o que se dará como regra, salvo previsão expressa em sentido contrário, tem o dever de consultar e atender às disposições da LGPD e àquelas eventualmente emitidas pela ANPD acerca de suas responsabilidades enquanto operador.

Quando o Tratamento for executado em nome de um Controlador, poderá se valer de outro operador (Sub-Operador) nas atividades de Tratamento realizadas em nome de um Controlador, salvo restrição específica apresentada pelo Controlador. Neste caso, havendo resistência pelo Controlador, poderá ser tornar inviável para a Ótima a manutenção do contrato, sendo esta causa considerada como justificadora de rescisão contratual.

Ao buscar um Operador para realizar tratamento de Dados em seu nome, a Ótima garante que o Operador siga as instruções e que seja estipulada de forma clara a natureza, a duração e a finalidade do Tratamento, o tipo de Dados Pessoais Tratados, as categorias dos titulares, as obrigações e os direitos do Controlador.

Os contratos firmados com Operadores deverão prever, entre outros aspectos:

- ✓ Trate os Dados Pessoais somente em instruções documentadas do Controlador, incluindo com referência a transferência dos Dados Pessoais a um terceiro país ou organização internacional, a não ser que seja obrigado a fazê-lo pela legislação a qual o Operador esteja submetido; nestes casos o Operador deverá informar ao Controlador todos os requerimentos legais antes do Tratamento, a menos que a lei proíba tais informações.
- ✓ Assegure que as pessoas autorizadas a tratar os Dados Pessoais tenham a obrigação contratual ou legal de manter sigilo e confidencialidade.
- ✓ Adote todas as medidas de segurança exigidas nos termos do Art. 46 da LGPD.
- ✓ Respeite as condições estabelecidas pela LGPD para subcontratar outro Operador, com a obrigação de garantir que a transferência internacional de dados para fora do Brasil será executada apenas para países considerados adequados com a legislação de privacidade local, e um documento contratual adequado seja previamente assinado entre o Operador e o Sub-Operador para garantir os direitos dos titulares.
- ✓ Adote, considerando a natureza do Tratamento, medidas técnicas e organizacionais apropriadas, na medida do possível, que permitam ao Controlador atender as requisições dos titulares no exercício de seus direitos, conforme previstos no Capítulo III da LGPD.
- ✓ Preste assistência ao Controlador para garantir a conformidade com obrigações relacionadas às medidas de Segurança (Capítulo VII da LGPD), Notificação e Comunicação de Incidente de Segurança de Dados (Art. 48 da LGPD) e DPIA (Art. 38 da LGPD). A Ótima na condição de operadora, quando requisitada ou responsável, sempre assistirá seus clientes (controladores de dados pessoais) com informações para que estes possam cumprir suas obrigações quanto a legislação vigente.
- ✓ Elimine ou devolva, a critério exclusivo do Controlador, todos os Dados Pessoais ao término da prestação dos serviços relacionados, deletando cópias existentes, a não ser que disposto expressamente em contrário na legislação aplicável para o armazenamento dos Dados Pessoais objeto do respectivo Tratamento.
- ✓ Disponibilize ao Controlador todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas na LGPD.

10.3 Transferência Internacional de Dados

Caso venha a ocorrer transferência internacional de dados pessoais, esta será realizada em conformidade com a Lei Geral de Proteção de Dados, observando as Resoluções da Autoridade Nacional de Proteção de Dados relativas ao tema, mediante utilização de mecanismos reconhecidos pela legislação, incluindo decisões de adequação, cláusulas-padrão contratuais, normas corporativas globais ou outros instrumentos aprovados pela ANPD.

10.4 Tratamento de dados em nome da Ótima

Atualmente, a Ótima não utiliza terceiros para tratamento de dados pessoais em seu nome.

Caso venha a utilizar, deverá garantir que tais terceiros sejam previamente avaliados quanto aos requisitos de segurança da informação e proteção de dados pessoais, incluindo:

- ✓ Avaliação de riscos (due diligence)
- ✓ Formalização contratual com cláusulas específicas de proteção de dados
- ✓ Monitoramento contínuo do cumprimento das obrigações estabelecidas

11. Controles e Ações exigidas pela Ótima aos Colaboradores e Responsáveis Diretos

As medidas técnicas e administrativas serão implementadas considerando o estado da técnica, os custos de implementação, a natureza, o contexto, as finalidades do tratamento e os riscos aos direitos e liberdades dos titulares.

O Controlador observa e atende às disposições contidas na LGPD e àquelas que venham a ser emitidas pela ANPD acerca das medidas de segurança aplicáveis às atividades de Tratamento. Considerando as condições existentes, os custos de implementação, a natureza, âmbito, contexto e finalidades do Tratamento, bem como o risco e impacto perante os direitos e liberdades dos titulares, o Controlador e o Operador devem implementar medidas técnicas e organizacionais destinadas a garantir um nível de segurança adequado, incluindo, entre outras, as medidas de Privacy by design (desde a concepção) e Privacy by default (por padrão).

O Controlador e o Operador devem:

- ✓ Rever e proteger todos os sistemas, identificação de aplicações e infraestruturas e acesso lógico.
- ✓ Rever e gerir de forma segura os Dados Pessoais e Dados Pessoais Sensíveis, com o objetivo de garantir uma elevada qualidade de dados e de forma que o Tratamento se limite ao necessário e ao adequado.
- ✓ Segregar os Dados Pessoais e perfilar usuários que lidem com Dados Pessoais, limitando acesso e atribuições de acordo com o estritamente necessário para execução de suas tarefas.
- ✓ Anonimizar e criptografar Dados Pessoais e Dados Pessoais Sensíveis. A escolha entre as 3 (três) opções deve ser a disponível ao Controlador e ao Operador.
- ✓ Assegurar permanentemente a confidencialidade, integridade, disponibilidade e resistência dos sistemas empregados nos tratamentos.
- ✓ Restaurar prontamente o acesso e disponibilidade dos Dados Pessoais em caso de incidentes de segurança.
- ✓ Testar, verificar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do Tratamento.
- ✓ Ao avaliar o nível adequado de segurança, devem ser considerados os riscos apresentados pelo Tratamento, particularmente em caso de conduta ilegal ou acidental que leve a destruição, perda, alteração, divulgação não autorizada ou ao acesso do Dado Pessoal transmitido, armazenado ou de outra forma tratado.
- ✓ A adesão a um código de conduta aprovado pela ANPD ou a um mecanismo de certificação aprovado em linha com as boas práticas de proteção de dados pode ser utilizado como elementos para demonstrar a conformidade com a LGPD.
- ✓ A Ótima, em caso de incidentes de segurança que venham causar violação de dados pessoais em sua estrutura, se compromete a notificar seus Clientes em um prazo máximo de 24 horas.

11.1 Gestão de Incidentes

A Ótima possui uma política formal de gestão de incidentes de segurança da informação, que inclui:

- ✓ Identificação, registro e classificação de incidentes
- ✓ Resposta e contenção de impactos
- ✓ Comunicação às partes interessadas e autoridades competentes
- ✓ Análise de causa raiz e implementação de ações corretivas
- ✓ Registro e monitoramento de lições aprendidas

Com o objetivo de assegurar que todos os incidentes de segurança da informação sejam identificados, avaliados e tratados de forma eficaz para minimizar o impacto sobre os ativos e para manter a confidencialidade, integridade e disponibilidade das informações.

Após a contenção do incidente, deverão ser implementadas medidas destinadas à mitigação dos impactos, restauração segura dos serviços e prevenção da recorrência.

A eficácia desta política impacta diretamente na continuidade dos negócios, que por si, determina sua importância. Quando aplicável, os incidentes envolvendo dados pessoais serão comunicados à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, conforme requisitos legais.

12. Direitos dos Titulares

O direito à privacidade e à proteção de Dados Pessoais devem ser considerados face a outros direitos fundamentais, de acordo com o princípio da proporcionalidade. O exercício dos direitos dependerá da adequada validação da identidade do solicitante, como medida destinada à prevenção de fraudes e proteção dos próprios titulares.

O Controlador assegura mecanismos adequados para possibilitar aos titulares o exercício dos direitos previstos na LGPD, observados os prazos legais, sem atrasos injustificados, por meio de canais acessíveis, transparentes e de fácil utilização. As respostas serão fornecidas imediatamente quando possível, ou no prazo legal de até 15 (quinze) dias, conforme a natureza da solicitação.

O Controlador tem o ônus de provar o pedido manifestamente excessivo ou não fundamentado. Além disso, o exercício de direitos é realizado de forma gratuita ao Titular e é responsável do Controlador adotar medidas técnicas e organizacionais para processar o exercício dos direitos do Titular.

São direitos dos Titulares, de acordo com a LGPD:

- ✓ Confirmação da existência de Tratamento.
- ✓ Acesso aos dados.
- ✓ Correção de dados incompletos, inexatos ou desatualizados.
- ✓ Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
- ✓ Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa.
- ✓ Eliminação dos Dados Pessoais tratados com o Consentimento.
- ✓ Informação sobre entidades públicas e privadas com as quais foi realizado o uso compartilhado de dados.
- ✓ Informação sobre a possibilidade de não fornecimento do consentimento e sobre as consequências da negativa.
- ✓ Revogação do consentimento.
- ✓ Revisão das decisões automatizadas tomadas unicamente com base no Tratamento automatizado de Dados Pessoais.
- ✓ Oposição a Tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD.

12.1 Confirmação e Direito de Acesso

O Titular tem o direito de ser informado de que um Tratamento relativo aos seus próprios dados está em andamento e, em caso de resposta afirmativa, obter acesso aos seus Dados Pessoais e receber uma cópia destes.

A confirmação de existência ou o acesso a Dados Pessoais serão providenciados em formato simplificado, imediatamente ou dentro do prazo de até 15 (quinze) dias por meio de declaração clara e completa, que indique: a origem dos dados e a finalidade do Tratamento, observados os segredos comercial e industrial, fornecida gratuitamente, contado da data do requerimento do Titular.

Os Dados Pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. As informações e os Dados Pessoais poderão ser fornecidos, a critério do Titular: por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa. A cópia dos Dados Pessoais deve ser fornecida ao Titular de forma gratuita.

12.2 Direito de Correção

O Titular tem o direito de obter do Controlador a correção de Dados Pessoais que lhe dizem respeito e que estejam incompletos, inexatos ou desatualizados.

12.3 Revogação do Consentimento e Eliminação

O Titular tem o direito de revogar o Consentimento anteriormente manifestado a qualquer momento mediante manifestação expressa, por procedimento gratuito e facilitado. O Titular também tem o direito de obter a eliminação dos Dados Pessoais tratados com o seu Consentimento.

O Controlador deve eliminá-los considerando a tecnologia disponível e os custos de implementação adotando medidas apropriadas.

Devem ser deletados quaisquer links, cópias ou reproduções de seus Dados Pessoais. Exceções somente poderão ser realizadas na medida em que o Tratamento seja necessário para:

- ✓ Cumprimento de obrigação legal ou regulatória pelo Controlador.
- ✓ Estudo por órgão de pesquisa, garantida, sempre que possível, a Anonimização dos Dados Pessoais.
- ✓ Transferência a terceiro, desde que respeitados os requisitos de Tratamento de dados disposto na LGPD.
- ✓ Uso exclusivo do Controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.
- ✓ O Controlador deve informar outros Controladores envolvidos no mesmo Tratamento de dados sobre a solicitação de eliminação.

12.4 Anonimização, bloqueio ou eliminação

O Titular tem o direito de obter do Controlador a Anonimização, Bloqueio ou Eliminação de Dados Pessoais:

- ✓ Desnecessários.
- ✓ Excessivos, ou tratados em desconformidade com o disposto na LGPD.
- ✓ Desse modo, através da técnica de Anonimização, um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, de modo que ocorra a desvinculação dos Dados Pessoais, não sendo possível identificar quem é o Titular.
- ✓ Por meio do Bloqueio dos Dados Pessoais, ocorrerá a suspensão temporária de qualquer operação de Tratamento, mediante guarda do dado pessoal ou do banco de dados.
- ✓ Já a Eliminação, prevê que um dado ou um conjunto de dados sejam excluídos do banco de dados da organização.

12.5 Portabilidade dos dados

O Titular tem direito a receber de forma estruturada Dados Pessoais fornecidos a um Controlador e tem o direito de transmitir tais dados para outro controlador, sem interferência do Controlador.

Ao exercer o direito à portabilidade de dados, o Titular tem o direito de obter a transmissão direta de Dados Pessoais, quando tecnicamente viável, de um Controlador ou outro.

12.6 Obtenção de informações sobre o compartilhamento de seus Dados

O Titular dos Dados Pessoais tem o direito de ter informações do Controlador sobre as entidades públicas e/ou privadas com as quais os seus Dados Pessoais tenham sido compartilhados.

O Titular dos Dados Pessoais tem o direito de ser informado sobre a possibilidade de não fornecer o seu consentimento bem como sobre as consequências da negativa. Como por exemplo, eventuais prejuízos, limitações de acesso, dentre outras consequências.

12.7 Revisão de Decisões Automatizadas

O Titular tem direito de solicitar a revisão de decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

O Controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

Em caso de não oferecimento dessas informações baseadas na observância de segredo comercial e industrial, a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios em Tratamento automatizado de Dados Pessoais.

12.8 Direito a Oposição quanto ao Tratamento dos Seus Dados

De acordo com o direito de oposição, o Titular dos Dados Pessoais poderá se opor ao Tratamento de seus Dados Pessoais com fundamento em uma das hipóteses de dispensa de Consentimento quando realizado em descumprimento à LGPD.

13. Integração ao Sistema de Gestão de Segurança da Informação

Esta Política integra o Sistema de Gestão de Segurança da Informação (SGSI) da Ótima, conforme a ISO/IEC 27001, estando alinhada aos objetivos estratégicos de segurança da informação e privacidade.

Seu cumprimento é monitorado continuamente por meio de auditorias internas, análise crítica da direção e melhoria contínua baseada no ciclo PDCA (Plan-Do-Check-Act).

A gestão de privacidade será continuamente revisada considerando alterações regulatórias, evolução tecnológica, riscos identificados, resultados de auditorias e oportunidades de melhoria.

A Ótima acompanha continuamente a evolução da legislação aplicável, das regulamentações, guias, orientações e demais atos normativos publicados pela Autoridade Nacional de Proteção de Dados (ANPD) e por outros órgãos competentes, promovendo, sempre que necessário, a atualização de seus processos, controles internos, políticas corporativas e práticas de governança em privacidade.

14. Monitoramento e Auditoria

A Ótima estabelece indicadores de desempenho para monitorar a eficácia dos controles de segurança e privacidade. São realizadas auditorias internas periódicas para avaliar a conformidade com esta Política e com as normas ISO 27001 e 27701. Os indicadores podem incluir, entre outros: número de incidentes, tempo de resposta, conformidade com treinamentos e resultados de auditorias. Esses resultados são analisados pela alta direção, visando a melhoria contínua dos processos.

15. Encarregado de Proteção de Dados

A Ótima disponibiliza canais oficiais para atendimento aos titulares de dados pessoais e comunicação com o Encarregado pelo Tratamento de Dados Pessoais.

Nosso Website: <https://otima.digital>

Contato do DPO: dpo@otima.digital

DPO: Fabio Manastarla Ferreira

16. Atualização

Esta Política será monitorada continuamente quanto à sua aderência à legislação aplicável, às regulamentações da ANPD, às normas internacionais adotadas pela organização e às melhores práticas de mercado, sendo revisada sempre que necessário para manter sua efetividade e conformidade.

17. Histórico de Atualizações

Elaboração / Revisão	Data	Versão	Escopo	Observação	Aprovação	Data
Fabio Ferreira	20/11/2019	1	Edição	N/A	Diretoria	20/11/2019
Fabio Ferreira	14/06/2021	2	Atualização	Atualização Item 12	Diretoria	14/06/2021
Fabio Ferreira	08/04/2022	3	Atualização	Atualização Item 12	Diretoria	08/12/2022
Fabio Ferreira	27/06/2023	4	Revisão	Sem Alterações	Diretoria	27/06/2023

Fabio Ferreira	02/05/2024	5	Revisão	Revisão Geral	Diretoria	02/05/2024
Fabio Ferreira	12/02/2025	6	Revisão	Sem alterações	Diretoria	12/02/2025
Fabio Ferreira	27/09/2025	7	Atualização	Atualização itens 6 e 11	Diretoria	27/09/2025
Fabio Ferreira	02/07/2026	8	Atualização	Revisão Geral	Diretoria	02/07/2026