Elaboração:	Análise Crítica/Aprovação:	Rev:	Data	Natureza das Alterações
Thales Rollo	Mariana Duardes	00	07/07/2025	Versão inicial

1. Apresentação

A **TELTEX TECNOLOGIA S.A** reconhece que quase todas as organizações tratam de dados pessoais (DP). Além disso, a quantidade e os tipos de dados pessoais (DP) tratados estão aumentando, assim como o número de situações em que uma organização precisa cooperar com outras organizações em relação ao tratamento de DP.

A **TELTEX TECNOLOGIA S.A** reconhece ainda que a proteção da privacidade no contexto do tratamento de DP é uma necessidade da sociedade, bem como um tópico de legislação e/ou regulamentação dedicada em todo o mundo, por isso estruturou seu Sistema de Gestão de Segurança da Informação (SGSI), de forma a permitir a adição de requisitos específicos sem a necessidade de desenvolver um novo Sistema de Gestão, mas considerando:

- uma estrutura de privacidade e os princípios estabelecidos em seu SGSI;
- conformidade com a Lei Brasileira de Proteção aos Dados Pessoais: Lei Geral de Proteção de Dados Pessoais (LGPD) Lei nº 13.709, de 14/08/2018.

A **TELTEX** se compromete em revisar a presente política sempre que ocorrer:

- Mudança legislativa relevante
- Incidente de segurança com impacto significativo
- Alteração substancial no modelo de negócios ou serviços prestados

Estas diretrizes devem ser lidas, compreendidas e seguidas pelos colaboradores, bem como provedores de produtos e serviços externos pertinentes, para que os principais ativos da **TELTEX**, incluindo informação, software e hardware, tenham o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

2. Escopo para aplicação

O escopo da presente Política se aplica à área de Tecnologia da Informação, Recursos Humanos e Suprimentos, no que se refere aos colaboradores, prestadores de serviços e provedores externos:

- **Prestadores de serviços de TI:** como empresas de hospedagem, suporte técnico, cloud computing, backup e recuperação de dados.
- **Consultorias e auditores externos:** que realizam avaliações, auditorias ou suporte à implementação do SGSI.
- **Fornecedores de software:** especialmente os que fornecem sistemas integrados, ERPs, CRMs ou ferramentas que lidam com dados corporativos.
- **Serviços de comunicação e transporte de dados:** como operadoras de telecomunicações ou correios que lidam com documentos confidenciais.
- **Serviços jurídicos e contábeis:** que acessam informações estratégicas, contratuais ou financeiras da empresa.

Para a correta aplicação da presente Política é necessário considerar os seguintes termos e definições:

- **sistema de gestão da segurança da informação SGSI**
  sistema de gestão da segurança da informação que considera conjunto de aplicações, serviços, ativos de tecnologia da informação ou outros componentes de manuseio de informações
- **dados pessoais DP**
  qualquer informação que (a) possa ser usada para identificar a pessoa natural à qual tal informação se relaciona ou (b) é ou pode ser direta ou indiretamente vinculada a uma pessoa natural
- **dado pessoal sensível**
  dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
- **titular de DP**
  pessoa natural a quem se referem os dados pessoais (DP)
- **operador de DP**
  parte interessada na privacidade, que faz o tratamento dos dados pessoais (DP) em benefício e de acordo com as instruções de um controlador de DP
- **controlador de DP**
  pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
- **tratamento de DP**
  toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração
- **incidente de segurança da informação**
  um ou múltiplos eventos de segurança da informação relacionados e identificados que podem prejudicar os ativos da organização ou comprometer suas operações

3. Público alvo

A presente Política se aplica a todos os colaboradores, prestadores de serviços e provedores externos, independentemente de serem residentes ou não no Brasil, incluindo suas coligadas e controladas, que estejam envolvidos em processos de negócios com a **TELTEX**, tais como: pré-qualificações e procedimentos de contratação direta, bem como aqueles que celebrem com a **TELTEX** instrumentos jurídicos em virtude de tais processos, independentemente de se tratar de processo de aquisição de bens tangíveis, intangíveis, contrato, convênio, termo de cooperação ou outro instrumento.

4. Procedimento

4.1 Condições para coleta e tratamento

Os dados pessoais (DP) coletados pela **TELTEX** possuem finalidade clara e legítima, como controle de acesso e suporte à garantia da segurança patrimonial, conforme contratado por seus clientes, não sendo permitido o uso para fins incompatíveis com os originais.

4.1.1 Dados coletados

Tipo de dado	Exemplos comuns em empresas de vigilância	Titular
Dados de identificação	Nome, CPF, RG, endereço, telefone	Colaboradores, Prestadores de Serviços, Usuários dos Clientes
Dados de acesso e localização	Horário de entrada/saída, áreas visitadas	
Dados visuais	Imagens de câmeras, vídeos, capturas	
Dados de comportamento	Padrões de movimentação, alertas gerados	
Dados biométricos (se aplicável)	Impressão digital, reconhecimento facial	Colaboradores, Prestadores de Serviços Internos

4.1.2 Acordos com o cliente

Nos contratos acordados com seus clientes, a **TELTEX** considera os papéis da organização em fornecer assistência com as obrigações do cliente (considerando a natureza do tratamento e a informação disponível para a organização), por meio de implementação de controles de segurança para o tratamento em suas dependências, tais como:

- Controles Organizacionais;
- Controles de Pessoas;
- Controles Físicos
- Controles Tecnológicos

No contexto da prestação de serviços de vigilância e monitoramento, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e com os requisitos da norma ISO/IEC 27701, o CLIENTE é o único responsável pela obtenção do consentimento dos titulares dos dados pessoais eventualmente coletados por meio de câmeras de vigilância, sistemas de biometria ou quaisquer outros dispositivos de captação instalados em suas dependências físicas.

Cabe ao CLIENTE garantir que a coleta e o tratamento desses dados sejam realizados de forma lícita, transparente e adequada, observando as bases legais aplicáveis, bem como os princípios da minimização, finalidade e segurança da informação.

A **TELTEX** como prestadora dos serviços atuará como operadora dos dados, conforme definido pela LGPD, limitando-se ao tratamento conforme instruções documentadas do CLIENTE.

Cabe ao CLIENTE manter registros que comprovem a obtenção do consentimento, quando aplicável, e assegurar que os titulares sejam devidamente informados sobre a finalidade da coleta, o período de retenção e os direitos que lhes assistem nos termos da legislação vigente.

4.2 Identificação e documentação do propósito

Considerando a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) e com os requisitos da norma internacional ISO/IEC 27701, que estende os controles da ISO/IEC 27001 para a gestão da privacidade da informação, no contexto das atividades de vigilância e monitoramento, o tratamento de dados pessoais pela **TELTEX** é vinculado à finalidades legítimas, específicas, explícitas e informadas ao titular pelo CLIENTE, conforme previsto no artigo 6º, inciso I da LGPD.

A **TELTEX** procura assegurar que cada operação de coleta, armazenamento, compartilhamento ou eliminação de dados esteja claramente associada a propósitos previamente definidos, de caráter legítimo, os quais incluem:

- Proteção patrimonial e segurança física de colaboradores, visitantes e instalações.
- Controle de acesso a áreas restritas por meio de sistemas de biometria ou identificação por imagem.
- Investigação de incidentes ou suporte à autoridade policial mediante requisição legal.
- Cumprimento de obrigações contratuais com clientes que contratam serviços de monitoramento.

4.2.1 Uso de marketing e propaganda

A exposição de soluções de vigilância e monitoramento em ambientes de demonstração (show-room) pode envolver a coleta de dados pessoais dos visitantes, como imagens captadas por câmeras, dados biométricos ou informações de contato fornecidas voluntariamente.
A TELTEX observa rigorosamente os princípios da **Lei Geral de Proteção de Dados Pessoais (LGPD)** e os controles definidos pela **ISO/IEC 27701** o uso desses dados para fins de marketing e propaganda.

Utilizamos como Boas Práticas:

- Exibir **avisos visuais** no show-room informando que há captação de imagens e dados.
- Disponibilizar **termos de consentimento** para visitantes que desejem receber comunicações de marketing.
- Evitar o uso de imagens de visitantes em materiais promocionais sem autorização expressa.
- Documentar todas as ações de tratamento de dados para fins de auditoria e conformidade.

4.3 Identificação de bases legais

A TELTEX justifica o tratamento com as seguintes bases legais previstas na LGPD:

4.3.1 Cumprimento de obrigação legal ou regulatória

A LGPD, em seu artigo 7º, inciso II, autoriza o tratamento de dados pessoais sem consentimento quando necessário para o cumprimento de obrigação legal ou regulatória pelo controlador.

No segmento de vigilância e monitoramento isso pode incluir:

- Atendimento a normas da segurança pública, como exigências da Polícia Federal para empresas de segurança privada.
- Armazenamento de imagens por tempo determinado, conforme exigido por leis estaduais ou municipais.
- Compartilhamento de dados com autoridades competentes, como em investigações criminais ou auditorias regulatórias.
- Controle de acesso a áreas restritas, quando exigido por normas de segurança do trabalho ou legislação de proteção patrimonial.

4.3.2 Execução de contrato

A base legal de execução de contrato (art. 7º, inciso V da LGPD) permite o tratamento de dados pessoais sem consentimento, desde que seja necessário para a execução de um contrato do qual o titular dos dados seja parte ou para procedimentos preliminares relacionados a esse contrato

No segmento de vigilância e monitoramento isso pode incluir:

- Cadastro de clientes para prestação de serviços de segurança privada
- Registro de visitantes em condomínios ou empresas monitoradas, quando previsto contratualmente
- Tratamento de imagens e dados biométricos para controle de acesso, conforme cláusulas contratuais
- Compartilhamento de dados com parceiros operacionais, como empresas de resposta rápida ou centrais de atendimento, quando previsto no contrato

NOTA – Tanto as bases legais "Execução de Contrato" quanto a "Obrigação Legal/Regulatória" dispensam o consentimento do titular dos dados pessoais, e se encontram documentadas na presente Política com clareza, incluindo:

- A finalidade específica
- A relação contratual existente
- Os dados tratados
- E os limites do uso, conforme o contrato

4.3.3 Exercício regular de direitos

Prevista no art. 7º, inciso VI da LGPD, essa base legal permite o tratamento de dados sem consentimento quando for necessário para:

- Defesa em processos judiciais, administrativos ou arbitrais
- Preservação de provas
- Resguardo do contraditório e da ampla defesa

As aplicações práticas para empresas de vigilância e monitoramento como a **TELTEX** incluem:

• Armazenar imagens de câmeras de segurança por tempo superior ao habitual, caso possam ser úteis em uma investigação ou processo judicial
• Compartilhar dados com autoridades policiais ou judiciais, mediante requisição formal
• Manter registros de acesso ou ocorrências para se defender em ações trabalhistas, civis ou criminais
• Preservar dados de visitantes ou colaboradores em caso de incidentes que possam gerar litígios

*** Exemplo:** Se um visitante sofre um acidente dentro de um condomínio monitorado, a empresa pode guardar as imagens e dados de acesso para se defender em eventual processo, sem precisar do consentimento do titular.

4.3.4 Proteção da vida ou da incolumidade física

Permite o tratamento de dados sem consentimento quando for necessário para:

"A proteção da vida ou da incolumidade física do titular ou de terceiro."

Ou seja, com o objetivo principal for evitar riscos, prevenir acidentes ou proteger pessoas em ambientes monitorados.

As aplicações práticas para empresas de vigilância e monitoramento como a **TELTEX** incluem:

• Monitoramento por câmeras em áreas comuns de condomínios, empresas ou instituições públicas
• Controle de acesso com biometria ou reconhecimento facial, para impedir entrada de pessoas não autorizadas
• Registro de visitantes e prestadores de serviço, com coleta de dados para garantir segurança
• Armazenamento de imagens e registros para investigação de furtos, agressões ou situações de emergência

NOTA – Essa base é válida somente ao tratamento proporcional e não invasivo, ou seja:
"A finalidade é legítima e a medida utilizada é adequada e proporcional, desde que não invada ambientes de privacidade e intimidade dos empregados, tais como refeitórios, banheiros e vestiários".

4.3.5 Tutela da saúde

A base legal da tutela da saúde (art. 7º, inciso VIII da LGPD) é voltada principalmente para o tratamento de dados pessoais sensíveis quando necessário para procedimentos realizados por profissionais da saúde, serviços de saúde ou autoridade sanitária.

No contexto das atividades da **TELTEX** que realiza vigilância e monitoramento, embora essa base legal não se aplique diretamente, pode ser invocada caso a empresa esteja envolvida em situações específicas que envolvam risco à saúde ou apoio a serviços médicos, como mas não se limitando à:

- Monitoramento em hospitais, clínicas ou unidades de saúde, onde os sistemas de vigilância apoiam diretamente a proteção de pacientes e profissionais
- Controle de acesso a áreas críticas de saúde, como salas de isolamento ou laboratórios, com uso de biometria ou câmeras
- Resposta a emergências médicas, onde o registro por câmeras pode ser usado para apoiar o atendimento ou investigação de incidentes de saúde

Exemplo: Serviços de monitoramento em um hospital pode tratar dados sensíveis (como imagens de pacientes) para proteger a integridade física deles ou apoiar ações sanitárias - nesse caso, a base da tutela da saúde pode ser considerada.

4.3.6 Interesse legítimo do controlador

O interesse legítimo do controlador é uma das bases legais mais relevantes e flexíveis da LGPD, especialmente para empresas como as de vigilância e monitoramento, conforme previsto no art. 7º, inciso IX da LGPD e permite o tratamento de dados pessoais sem consentimento, desde que:

- O tratamento seja necessário para atender aos interesses legítimos do controlador ou de terceiros; e
- Não viole os direitos e liberdades fundamentais do titular dos dados.

No contexto de vigilância e monitoramento, o interesse legítimo pode ser usado em situações, como:

- **Segurança patrimonial:** gravação de imagens em áreas comuns para prevenir furtos ou invasões
- **Controle de acesso:** registro de entrada e saída de pessoas em ambientes monitorados
- **Proteção de funcionários e clientes:** uso de câmeras para garantir integridade física
- **Investigação de incidentes:** análise de imagens para apuração de eventos internos

4.4 Obtenção de consentimento

No contexto da prestação de serviços de vigilância e monitoramento, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e com os requisitos da norma ISO/IEC 27701, o CLIENTE é o único responsável pela obtenção do consentimento dos titulares dos dados pessoais eventualmente coletados por meio de câmeras de

vigilância, sistemas de biometria ou quaisquer outros dispositivos de captação instalados em suas dependências físicas.

NOTA – Tanto as bases legais "Execução de Contrato" quanto a "Obrigação Legal/Regulatória" dispensam o consentimento do titular dos dados pessoais, e se encontram documentadas na presente Política com clareza, incluindo:

- A finalidade específica
- A relação contratual existente
- Os dados tratados
- E os limites do uso, conforme o contrato

4.4.1 Casos aplicáveis para registro do consentimento

4.4.1.1 Monitoramento em áreas privadas ou sensíveis

- **Exemplo:** câmeras em ambientes como vestiários, salas de descanso ou áreas de uso restrito
- **Justificativa:** o tratamento pode afetar diretamente a privacidade do titular, exigindo consentimento explícito

4.4.1.2 Uso de dados para finalidades secundárias

- **Exemplo:** utilizar imagens gravadas para fins de marketing, treinamento interno ou divulgação institucional
- **Justificativa:** essas finalidades não estão diretamente ligadas à execução do contrato ou obrigação legal

4.4.1.3 Tratamento de dados sensíveis sem respaldo legal específico

- **Exemplo:** uso de **biometria** para controle de acesso em locais onde não há exigência legal ou contratual
- **Justificativa:** dados biométricos são sensíveis e exigem consentimento, salvo se houver outra base legal clara

4.4.1.4 Compartilhamento com terceiros fora do escopo contratual

- **Exemplo:** envio de dados para parceiros comerciais, empresas de tecnologia ou plataformas externas
- **Justificativa:** se não houver base legal como execução de contrato ou legítimo interesse, o consentimento é necessário

4.4.1.5 Gravação de áudio em conjunto com vídeo

- **Exemplo:** sistemas de CFTV que capturam som ambiente
- **Justificativa:** o áudio pode revelar informações pessoais não visíveis, exigindo consentimento em alguns contextos

4.5 Avaliação de impacto de privacidade

O **FORM-SGSI-05.34.01Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** é uma exigência prevista na **Lei Geral de Proteção de Dados (LGPD)**, especificamente nos **artigos 5º, inciso XVII, e 38 da Lei nº 13.709/2018**, constituindo uma ferramenta estratégica que ajuda o controlador a **avaliar os riscos** e **documentar as medidas de mitigação** em operações de tratamento de dados que possam representar **alto risco aos direitos e liberdades dos titulares**.

Com base nos riscos avaliados em seu **FORM-SGSI-06.1.02 Análise, Avaliação e Tratamento de Riscos de SGSI**, a **TELTEX** avalia especificamente o impacto de riscos à privacidade dos pessoais com os quais opera, considerando:

a) Identificação do controlador e encarregado
b) Descrição detalhada da operação de tratamento
c) Finalidade do tratamento
d) Base legal utilizada
e) Natureza dos dados tratados (inclusive se são sensíveis)
f) Avaliação dos riscos aos titulares
g) Medidas de segurança e mitigação adotadas
h) Consultas realizadas com partes interessadas
i) Justificativa da necessidade do tratamento
j) Inventário de dados e sistemas envolvidos
k) Análise de conformidade com princípios da LGPD
l) Aprovação interna e versão do documento

A ANPD (Autoridade Nacional de Proteção de Dados) recomenda a elaboração do RIPD especialmente quando:

- Há tratamento de dados sensíveis
- O tratamento envolve grande volume de dados
- Pode haver impacto significativo aos direitos dos titulares
- São utilizados tecnologias inovadoras, como biometria ou reconhecimento facial

4.6 Contratos com operadores de DP / Controlador conjunto de DP

A **TELTEX** recomenda aos operadores de DP tratando DP em seu nome que na medida do possível econômica e tecnicamente implemente os controles apropriados especificados no **Anexo** do presente documento, levando em conta o processo de avalição de riscos de segurança da informação e o escopo do tratamento de DP realizado pelo operador de DP.

Se o operador de DP decidir que não pode ou não deseja implementar nenhum dos controles do **Anexo**, a **TELTEX** pode solicitar que ela justifique a sua exclusão.

Um contrato pode estabelecer as responsabilidades de cada parte diferentemente, podendo ou não citar os controles considerados incluídos na informação documentada, determinando os papéis e responsabilidades para o tratamento de DP de forma transparente.

Um acordo com um controlador conjunto de DP pode incluir (esta lista não é definitiva nem exaustiva):

a) propósito do compartilhamento de DP/relacionamento do controlador conjunto de DP;
b) identidade das organizações (controladores de DP) que são parte do relacionamento do controlador conjunto de DP;
c) categorias de DP a serem compartilhadas e/ou transferidas e tratadas com base no acordo;
d) visão global das operações de tratamento (por exemplo, transferência, uso);

e) descrição dos respectivos papéis e responsabilidades;
f) responsabilidade pela implementação técnica e organizacional das medidas de segurança para proteção de DP;
g) definição de responsabilidade no caso de uma violação de DP (por exemplo, quem irá notificar, quando e informações mútuas);
h) termos de retenção e/ou descarte de DP;
i) responsabilidades cíveis por falha na conformidade com acordo;
j) como as obrigações dos titulares de DP são atendidas;
k) como fornecer aos titulares de DP informações que cubram a essência dos acordos entre os controladores conjuntos de DP;
l) como os titulares de DP podem obter outras informações que eles têm direito a receber;
m) um ponto de contato para os titulares de DP.

4.7 Registros relativos ao tratamento de DP

A **TELTEX** mantém por meio de seu **FORM-SGSI-06.1.01Inventário de Informações SGSI** uma lista das atividades de tratamento do DP que realiza, incluindo:

a) tipo de tratamento;
b) propósitos para o tratamento;
c) uma descrição das categorias de DP e dos titulares de DP (por exemplo, crianças);
d) as categorias de destinatário para quem o DP tem sido ou será divulgado, incluindo os destinatários em outros países ou organizações internacionais;
e) uma descrição geral das medidas de segurança técnica e organizacional; e
f) um relatório de Avaliação de Impacto de Privacidade (ver **FORM-SGSI-05.34.01Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**).

NOTA – Tanto as bases legais "Execução de Contrato" quanto a "Obrigação Legal/Regulatória" dispensam o consentimento do titular dos dados pessoais, e se encontram documentadas na presente Política com clareza, incluindo:

- A finalidade específica
- A relação contratual existente
- Os dados tratados
- E os limites do uso, conforme o contrato

4.8 Obrigações dos titulares de DP

A **TELTEX**, conforme os requisitos legais, regulamentares e/ou de negócio considerando a informação fornecida pelo titular de DP e conforme o tipo de informação fornecida, solicita aos titulares com os quais opera DP:

a) **Manter seus dados atualizados:** Isso ajuda os controladores a manterem a base de dados correta e evita problemas com comunicação ou prestação de serviços.
b) **Evitar compartilhamento excessivo de dados:** Ter consciência sobre quais dados está fornecendo e para quem, especialmente em ambientes digitais.
c) **Reportar irregularidades:** Caso perceba que seus dados estão sendo usados de forma indevida, o titular pode acionar a empresa responsável ou até mesmo a Autoridade Nacional de Proteção de Dados (**ANPD**).

d) **Conduta dentro da legalidade:** Não se envolver em atividades que sejam ilegais ou contrárias à boa fé a à ordem pública.
e) **Ameaças cibernéticas:** Não causar danos aos sistemas físicos (hardwares) e lógicos (softwares) da **TELTEX**, de seus fornecedores ou terceiros, para introduzir ou disseminar vírus informáticos ou quaisquer outros sistemas de hardware ou software que sejam capazes de causar danos anteriormente mencionados.
f) **Aos colaboradores, prestadores de serviços e provedores externos:** Não difundir propaganda ou conteúdo de natureza racista, xenofóbica, ou sites de apostas, jogos de sorte e azar, qualquer tipo de pornografia ilegal, de apologia ao terrorismo ou contra os direitos humanos.

4.9 Mecanismos para modificar ou cancelar o consentimento / Acesso, correção e/ou exclusão

A **TELTEX** informa aos titulares de DP por meio da presente Política sobre os seus direitos relativos ao cancelamento do consentimento (que podem variar por jurisdição) a qualquer tempo, e forneça o mecanismo para fazer isto.

O mecanismo usado pela **TELTEX** para cancelamento é por meio do e-mail:
ti@teltex.com.br

As comunicações por meio deste endereço eletrônico permitem:
- Modificar o consentimento, para incluir a colocação de restrições sobre o tratamento de DP, o que pode incluir restrição ao controlador de DP para excluir o DP em alguns casos.
- Solicitar para cancelar ou mudar o consentimento de uma forma similar ao registro do consentimento propriamente dito.

NOTA Algumas jurisdições impõem restrições sobre quando e como um titular de DP pode modificar ou cancelar o seu consentimento.

Uma vez que a **TELTEX** utiliza **apenas o e-mail acima como canal de comunicação**, visando garantir que os titulares de dados possam exercer seus direitos previstos na LGPD, como acesso e correção com segurança e transparência, são adotados procedimentos de autenticação, tais como:
a) Solicitar informações mínimas para confirmar a identidade do titular (ex: nome completo, CPF, e-mail cadastrado).
b) Evitar pedir dados sensíveis por e-mail, e nunca enviar dados pessoais sem confirmação da identidade

4.9.1 Resposta estruturada e dentro do prazo

Solicitações legítimas, incluindo pedidos para uma cópia do DP tratado, ou solicitação para apresentar uma queixa são tratadas dentro dos tempos de respostas apropriados, embora o titular de DP não possua direito irrestrito a cópias integrais de documentos, bancos de dados ou sistemas onde esses dados estão inseridos.

NOTA Se os registros contendo DP contêm dados de outros titulares, segredos comerciais ou informações protegidas por sigilo legal (como bancário, fiscal ou profissional), o controlador pode negar o fornecimento da cópia para proteger esses direitos.

A LGPD exige que o controlador responda às solicitações em prazo razoável (geralmente até 15 dias), fornecendo as seguintes informações:
Quais dados estão armazenados
Finalidade do tratamento
Possibilidade de correção ou exclusão
Informações sobre compartilhamento com terceiros, se houver

NOTA Embora o **Artigo 18** da LGPD garanta ao titular de DP o direito de solicitar a eliminação dos dados pessoais tratados com seu consentimento, essa eliminação **não se aplica** quando há exceções previstas no **Artigo 16**, que estabelece fundamentos para manutenção dos dados (ver **Anonimização e exclusão de DP ao final do tratamento** na presente Política).

4.10 Obrigações dos controladores de DP para informar aos terceiros

A **TELTEX** se compromete em informar a eventuais terceiros com quem o DP foi compartilhado sobre qualquer modificação, cancelamento ou desaprovação pertinente ao DP compartilhado, implementando comunicações via e-mail como mecanismo para fazê-lo.

A **TELTEX** ainda assegura que quaisquer cópias de DP fornecidas para um titular de DP estejam especificamente relacionadas com aquele titular de DP por meio dos procedimentos de autenticação mencionados no item **4.9** da presente Política.

A **TELTEX** possui a capacidade de retornar, transferir e/ou descartar DP de uma maneira segura. Arquivos temporários criados como um resultado do tratamento de DP pela **TELTEX** são descartados (por exemplo, apagados ou destruídos) seguindo o procedimento **SP.TI.DOC.004 Exclusão (Descarte) de informações**, dentro de um período especificado.

DP tratados podem ser apagados (pela **TELTEX** e quaisquer de seus subcontratados) do ponto onde eles estão armazenados, incluindo para os propósitos de cópias de segurança e continuidade dos negócios, tão logo eles não sejam mais necessários, para os propósitos identificados do cliente, exceto onde essa eliminação **não se aplica** conforme exceções previstas no **Artigo 16 da LGPD**, que estabelece fundamentos para manutenção dos dados (ver **Anonimização e exclusão de DP ao final do tratamento** na presente Política).

4.11 Privacy by Design e Privacy by Default

A **TELTEX** adota estes dois conceitos, pilares fundamentais da **LGPD** e também da **GDPR** (regulamento europeu), como forma de garantir que a **proteção de dados pessoais** seja levada a sério desde o início de qualquer projeto ou operação.

4.11.1 Privacy by Design (Privacidade desde a concepção)

Preconiza que a privacidade deve ser incorporada desde o início de qualquer processo, sistema, produto ou serviço que envolva dados pessoais. Ou seja:

- A proteção de dados não é um complemento, mas sim parte estrutural do projeto.

- Desde o planejamento, já se pensa em minimização de dados, segurança da informação, controle de acesso, e transparência.

Exemplo: ao desenvolver um sistema de monitoramento, a empresa já define que só serão coletados os dados estritamente necessários, e que haverá criptografia e controle de acesso desde o primeiro dia.

4.11.2 Privacy by Default (Privacidade por padrão)

Todas as configurações e práticas padrão de um sistema ou serviço priorizam a privacidade, sem exigir que o titular precise ajustar nada. Isso inclui:

- Coletar apenas os dados necessários para a finalidade legítima.
- Configurações padrão devem ser as mais restritivas em termos de compartilhamento e exposição.
- O tratamento de dados deve ser limitado ao mínimo necessário para cumprir a finalidade.

Exemplo: um aplicativo que, por padrão, não compartilha localização, não envia notificações promocionais, e não armazena dados sensíveis, a menos que o usuário autorize (exceto os casos previstos em lei; ver item **4.4** da presente Política).

4.12 Precisão e qualidade

A **TELTEX** busca assegurar que o DP é preciso, completo e atualizado, como é necessário para os propósitos aos quais ele é tratado, por meio do ciclo de vida do DP, obedecendo à instruções e procedimentos documentados "DOC.SGQ" e "DOC.SGSI".

Mecanismos para acesso, correção e/ou exclusão de DP são disponibilizados conforme item **4.9** da presente Política.

4.13 Controles de transmissão de DP

A **TELTEX** e seus subcontratados operam com DP transmitidos sobre uma rede de transmissão de dados sob controles apropriados conforme sua **FORM-SGSI-06.1.03 Declaração de Aplicabilidade,** projetados para assegurar que os dados alcancem seus destinos pretendidos.

A transmissão de DP é controlada para assegurar que somente pessoas autorizadas tenham acesso a sistemas de transmissão e sigam os processos apropriados (incluindo a retenção de dados de auditoria), de forma a garantir que DP sejam transmitidos sem comprometimento para os destinatários corretos.

4.14 Anonimização e exclusão de DP ao final do tratamento

Embora o **Artigo 18** da LGPD garanta ao titular de DP o direito de solicitar a eliminação dos dados pessoais tratados com seu consentimento, essa eliminação **não se aplica** quando há exceções previstas no **Artigo 16**, que estabelece os seguintes fundamentos para **manutenção dos dados**:

Art. 16 – O controlador poderá manter os dados pessoais mesmo após o término do tratamento nas seguintes hipóteses:

- I – cumprimento de obrigação legal ou regulatória pelo controlador;

- II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei;
- IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que os dados sejam anonimizados.

A **TELTEX** e seus clientes estão cobertos pelas bases legais "Execução de Contrato" e "Obrigação Legal/Regulatória";
No segmento de vigilância e monitoramento isso pode incluir:

- Atendimento a normas da segurança pública, como exigências da Polícia Federal para empresas de segurança privada.
- Armazenamento de imagens por tempo determinado, conforme exigido por leis estaduais ou municipais.
- Compartilhamento de dados com autoridades competentes, como em investigações criminais ou auditorias regulatórias.
- Controle de acesso a áreas restritas, quando exigido por normas de segurança do trabalho ou legislação de proteção patrimonial.

NOTA A **TELTEX** não é obrigada a anonimizar os dados após o tratamento caso:
- possa eliminá-los completamente após o término da finalidade.
- precise manter os dados por obrigação legal ou regulatória (LGPD Art. 16, incisos I e II).
- o uso dos dados continua sendo legítimo, como em estudos por órgãos de pesquisa (com anonimização sempre que possível).

4.15 Identificando as bases para a transferência de DP entre jurisdições

A **TELTEX** é uma empresa brasileira do segmento de vigilância e monitoramento que utiliza plataformas como Google Suite®, Gupy®, Segware®, Digifort®, InvGate®, Gruppen® e Tim Monitor®, muitas das quais operam com servidores ou suporte técnico fora do Brasil, mas que seguem igualmente as regras da **LGPD** para transferência internacional de dados pessoais.

A transferência internacional de dados está regulamentada pelos **Artigos 33** a **36** da **LGPD**, e **Resolução CD/ANPD nº 19/2024**, que clarifica a segurança jurídica para essas operações.

A **TELTEX** pode transferir dados para outras jurisdições com base em uma das seguintes situações permitidas pela LGPD:

1. **País com nível de proteção adequado**
   - A ANPD pode reconhecer que o país de destino oferece proteção equivalente à brasileira.
     Exemplo: Japão, Suíça e Coreia do Sul já têm reconhecimento de adequação pela União Europeia — o Brasil pode seguir critérios semelhantes.
2. **Cláusulas contratuais padrão (CCPs)**
   - A empresa pode adotar **modelos de contrato aprovados pela ANPD** que garantem proteção aos dados transferidos.
     Isso é útil para plataformas como Google Suite ou Gupy, que operam globalmente.
3. **Normas corporativas globais (BCRs)**

- Para grupos empresariais com presença internacional, é possível adotar regras internas corporativas que assegurem o tratamento adequado dos dados.

4. **Execução de contrato ou obrigação legal**
   - Se a transferência for necessária para cumprir contrato com o titular ou atender a uma obrigação legal, ela é permitida.
5. **Proteção da vida ou da integridade física**
   - Em situações emergenciais, como segurança patrimonial, a transferência pode ocorrer para proteger o titular ou terceiros.

No segmento de vigilância e monitoramento isso pode incluir requisitos adicionais:

- **FORM-SGSI-05.34.01Relatório de Impacto à Proteção de Dados Pessoais (RIPD),** exigido especialmente se houver tratamento de dados sensíveis (como imagens de câmeras).
- Garantia de que os dados transferidos estejam protegidos por medidas técnicas e organizacionais adequadas, conforme **FORM-SGSI-06.1.03 Declaração de Aplicabilidade**.
- Manter transparência com os titulares, informando sobre a transferência na presente **Política de Proteção à Privacidade de Dados Pessoais**.

4.16 Divulgações legalmente obrigatórias de DP

A **TELTEX** rejeita quaisquer solicitações para a divulgação de DP que não sejam legalmente obrigatórias, tais como:

- **Cumprimento de obrigação legal ou regulatória**
  Exemplo: fornecimento de dados a órgãos como **Polícia Civil, Ministério Público ou Poder Judiciário**.
  Pode incluir:
  - Imagens de câmeras de segurança
  - Registros de acesso (nome, horário, local)
  - Dados de identificação (CPF, RG, endereço)
- **Execução de contrato**
  Se o controlador dos dados solicita os dados contratados (ex: histórico de acesso ou imagens), a empresa deve fornecer.
  Também pode ocorrer em auditorias ou fiscalizações contratuais.
- **Decisão judicial ou administrativa**
  A empresa pode ser obrigada a divulgar dados mediante mandado judicial ou determinação da ANPD.
  Exemplo: investigação de furto, violência ou fraude.
- **Proteção da vida ou da integridade física**
  Em casos de emergência, a divulgação pode ser feita para proteger o titular ou terceiros.
  Exemplo: fornecimento de imagens para localizar uma pessoa desaparecida.

4.16.1 Tipos de dados que podem ser exigidos:

Tipo de dado	Exemplos comuns em empresas de vigilância	Titular
Dados de identificação	Nome, CPF, RG, endereço, telefone	Colaboradores, Prestadores de Serviços, Usuários dos Clientes
Dados de acesso e localização	Horário de entrada/saída, áreas visitadas	
Dados visuais	Imagens de câmeras, vídeos, capturas	
Dados de comportamento	Padrões de movimentação, alertas gerados	
Dados biométricos (se aplicável)	Impressão digital, reconhecimento facial	Colaboradores, Prestadores de Serviços Internos

4.17 Contratação de subcontratado para tratar DP

A **TELTEX,** se necessário, somente contrata um subcontratado para tratar DP com base no contrato do cliente. A **TELTEX** mantém um contrato por escrito com quaisquer subcontratados que ela utilize para o tratamento de DP, atuando em seu nome, podendo requerer que o subcontratado implemente controles apropriados como especificado no **Anexo**.

Conforme cláusulas contratuais específicas, a **TELTEX** pode vir a informar o cliente sobre quaisquer alterações pretendidas relativas à adição ou substituição de subcontratados para tratar DP, dando assim ao cliente a oportunidade de se opor a essas alterações.

4.18 Divulgações que a TELTEX realiza

4.18.1 Política de Privacidade

A presente Política está disponível no endereço eletrônico:

https://teltex.com.br

Esta Política contém:

- Quais dados são coletados (ex: imagens, biometria, nome, CPF)
- Finalidade do tratamento (ex: segurança, controle de acesso)
- Compartilhamento com terceiros (ex: uso de Digifort, Segware, Gupy)
- Tempo de retenção dos dados
- Direitos dos titulares e como exercê-los

4.18.2 Nome e contato do Encarregado de Dados (DPO)

O **DPO,** sigla para **Data Protection Officer**, é chamado na **LGPD** de **Encarregado pelo Tratamento de Dados Pessoais,** figura central na governança da privacidade dentro das organizações.

Uma vez que a TELTEX trata dados de imagem, considerados dados sensíveis sob certo ponto de vista, ela designou para esta função:

Mariana Duardes - ti@teltex.com.br
Rua França Pinto, 1089
Vila Mariana - São Paulo - SP
CEP: 04016-030
Tel: +55 (11) 3840.6400

4.18.3 Canal de atendimento ao titular

A **TELTEX** disponibiliza os canais acima para solicitar acesso, correção ou exclusão de dados, modificar consentimento (observar item **4.4** da presente Política) e reclamar sobre uso indevido.

4.18.4 Avisos de coleta em ambientes monitorados

A **TELTEX** sinaliza apropriadamente, de forma visível, os ambientes com câmeras ou sensores em suas instalações
Exemplo: "Este local é monitorado por câmeras. As imagens podem ser armazenadas e são protegidas nos termos da lei."

NOTA A responsabilidade sobre sinalização nas instalações do cliente é de responsabilidade do cliente.

4.18.5 Notificação de incidentes de segurança

Em caso de vazamento ou acesso indevido, a TELTEX procede conforme **SP.TI.DOC.002 Gestão de Incidentes de Segurança da Informação**, contemplando:

- Identificação e Detecção
- Notificação e Comunicação
- Classificação e Avaliação
- Resposta e Contenção
- Remediação e Recuperação
- Registro e Documentação
- Aprendizado e Melhoria Contínua

Conforme **artigo 48** da **LGPD**, se o incidente representar risco ou dano relevante aos direitos desses titulares, a **TELTEX** notifica a **ANPD** em até **3 dias úteis** após tomar conhecimento do incidente, podendo informar aos titulares afetados pelo e-mail ti@teltex.com.br. Conforme apropriado a **TELTEX** pode divulgar as medidas corretivas adotadas.

4.18.5.1 Critérios que exigem notificação:

A comunicação é obrigatória quando o incidente envolve:

- Dados pessoais **sensíveis**
- Dados de **crianças, adolescentes ou idosos**
- Informações **financeiras, biométricas** ou protegidas por **sigilo legal**
- Tratamento de dados em **larga escala**

ANEXO

Cláusula ISO 27701	Controle	Descrição
B.8.2 Condições para coleta e tratamento Objetivo: Documentar e determinar que o tratamento é lícito, com base legal, conforme as jurisdições aplicáveis e com propósitos legítimos e claramente definidos.		
B.8.2.1	Acordos com o cliente	A organização deve assegurar, onde pertinente, que o contrato para tratar DP considera os papéis da organização em fornecer assistência com as obrigações do cliente (considerando a natureza do tratamento e a informação disponível para a organização).
B.8.2.2	Propósitos da organização	A organização deve assegurar que os DP tratados em nome do cliente sejam apenas tratados para o propósito expresso nas instruções documentadas do cliente.
B.8.2.3	Uso de marketing e propaganda	A organização não pode utilizar os DP tratados sob um contrato para o propósito de marketing e propaganda, sem o estabelecimento de que um consentimento antecipado foi obtido do titular de DP apropriado. A organização não pode fornecer este consentimento como uma condição para o recebimento do serviço.
B.8.2.4	Violando instruções	A organização deve informar ao cliente se, na sua opinião, uma instrução de tratamento viola uma regulamentação e/ou legislação aplicável.
B.8.2.5	Obrigações do cliente	A organização deve fornecer ao cliente informações apropriadas de tal modo que o cliente possa demonstrar compliance com suas obrigações.
B.8.2.6	Registros relativos ao tratamento de DP	A organização deve determinar e manter os registros necessários para apoiar a demonstração do compliance com suas obrigações (como especificado no contrato aplicável) para tratamento de DP realizado em nome do cliente.
B.8.3 Obrigações para os titulares de DP Objetivo: Assegurar que os titulares de DP sejam providos com informações apropriadas sobre o tratamento de seus DP, e que estejam de acordo com quaisquer outras obrigações aplicáveis para os titulares de DP relativas ao tratamento de seus DP.		
B.8.3.1	Obrigações para os titulares de DP	A organização deve fornecer ao cliente meios para estar em compliance com suas obrigações relativas aos titulares de DP.

Cláusula ISO 27701	Controle	Descrição
B.8.4 Privacy by design e Privacy by Default Objetivo: Assegurar que processos e sistemas sejam projetados de forma que a coleta e o tratamento de DP (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.		
B.8.4.1	Arquivos temporários	A organização deve assegurar que os arquivos temporários criados como um resultado do tratamento de DP sejam descartados (por exemplo, apagados ou destruídos) seguindo os procedimentos documentados, dentro de um período especificado e documentado.
B.8.4.2	Retorno, transferência ou descarte de DP	A organização deve fornecer a capacidade de retornar, transferir e/ou descartar DP de uma maneira segura. Deve também tornar sua política disponível para o cliente.
B.8.4.3	Controles de transmissão de DP	A organização deve sujeitar DP transmitidos sobre uma rede de transmissão de dados a controles apropriados projetados, para assegurar que os dados alcancem seus destinos pretendidos.
B.8.5 Compartilhamento, transferência e descarte de DP Objetivo: Determinar se e documentar quando DP são compartilhados, transferidos para outras jurisdições ou terceiros e/ou divulgados, de acordo com as obrigações aplicáveis.		
B.8.5.1	Bases para a transferência de DP entre jurisdições	A organização deve informar ao cliente em um tempo hábil sobre as bases para a transferência de DP entre jurisdições e de qualquer mudança pretendida nesta questão, de modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o contrato.
B.8.5.2	Países e organizações internacionais para os quais o DP podem ser transferidos	A organização deve especificar e documentar os países e as organizações internacionais para os quais DP possam, possivelmente, ser transferidos.
B.8.5.3	Registros de DP divulgados para terceiros	A organização deve registrar a divulgação de DP para terceiros, incluindo quais DP foram divulgados, para quem e quando.
B.8.5.4	Notificação de solicitações de divulgação de DP	A organização deve notificar ao cliente sobre quaisquer solicitações legalmente obrigatórias para a divulgação de DP.
B.8.5.5	Divulgações legalmente obrigatórias de DP	A organização deve rejeitar quaisquer solicitações para a divulgação de DP que não sejam legalmente obrigatórias, consultar o cliente em questão antes de

Cláusula ISO 27701	Controle	Descrição
		realizar quaisquer divulgações do DP e aceitar quaisquer solicitações contratualmente acordadas para a divulgação de DP, que sejam autorizadas pelo respectivo cliente.
B.8.5.6	Divulgação de subcontratados usados para tratar DP	A organização deve divulgar para o cliente qualquer uso de subcontratados para tratar DP, antes do uso.
B.8.5.7	Contratação de um subcontratado para tratar DP	A organização deve somente contratar um subcontratado para tratar DP com base no contrato do cliente.
B.8.5.8	Mudança de subcontratado para tratar DP	A organização deve, no caso de ter uma autorização geral por escrito, informar o cliente de quaisquer alterações pretendidas relativas à adição ou substituição de subcontrata-dos no tratamento de DP, dando assim ao cliente a oportunidade de se opor a essas alterações.
B.8.6 Canais, Prazos e Transparência Digital		
B.8.6.1	Canais múltiplos para titulares de DP	A organização deve disponibilizar ao menos dois canais para que os titulares de DP possam exercer seus direitos previstos na legislação, como: • E-mail corporativo • Endereço Físico • Telefone
B.8.6.2	Prazo para atendimento de solicitações dos titulares	A organização deve responder às solicitações legítimas dos titulares de DP no prazo máximo de 15 (quinze) dias corridos, contados a partir da comprovação da identidade do requerente conforme item **4.9.1** da presente Política.
B.8.6.3	Política de Cookies e Aviso de Privacidade Digital	A organização deve manter disponível, em seu website institucional, as seguintes documentações públicas: • Política de Cookies: detalhando os tipos utilizados, suas finalidades e opções de consentimento conforme conforme https://teltex.com.br/politica-de-privacidade.

Cláusula ISO 27701	Controle	Descrição
		• Aviso de Privacidade Digital: explicando o tratamento de dados em ambiente digital, inclusive no acesso ao site, formulários e serviços online. Tais documentos devem estar acessíveis por hiperlink no rodapé da página inicial, com linguagem clara e objetiva.
B.8.6.4	Revisão periódica da Política de Privacidade	A organização deve revisar formalmente a presente política conforme **SP.TI.DOC.010 Controle de Informação Documentada no SGSI**, ou sempre que ocorrer: • Mudança legislativa relevante • Incidente de segurança com impacto significativo • Alteração substancial no modelo de negócios ou serviços prestados A versão revisada deverá conter: • Número da revisão • Data de aprovação • Natureza das alterações • Responsável pela atualização