Política de Privacidade Cesla
Cesla Privacy Policy

Versão 2.2 | 22 de Agosto de 2025
Responsável Técnico: CPO – Silvia Adriana Silvestrini
Aprovador Institucional: CEO – Cleber Candido Eduardo
Status do documento: Aprovado
Uso Interno - Documento Confidencial

Version 2.2 | Aug 22, 2025
Technical Responsible: CPO – Silvia Adriana Silvestrini
Executive Approver: CEO – Cleber Candido Eduardo
Document Status: Approved
Internal Use / Confidential Document

Sumário

Controle de versionamento – Política de Privacidade Cesla
Version Control – Cesla Privacy Policy

Emissão Inicial / Document creation – V1.0		
Data: **Creation Date:**	June, 2021	**Comentários / Conteúdo revisado** **Comments / Revised Content**
Criado por: **Created by:**	Paulo Rodrigues - CTO	• Emissão inicial | Document creation
Revisado por: **Reviewed by:**	Silvia Adriana Silvestrini – CPO	
Aprovado por: **Approved by:**	Cleber Candido Eduardo – CEO	

Versão / Version V2.0		
Data: **Creation Date:**	May 2, 2025	**Comentários / Conteúdo revisado** **Comments / Revised Content**
Criado por: **Created by:**	Comitê de Tecnologia Cesla | Cesla Technology Committee	• Revisão geral de lay-out e conteúdo | Layout and content review • Elaboração do Documento – Versão Bilíngue (Português/Inglês) | Bilingual Document Preparation (Portuguese/English)
Revisado por: **Reviewed by:**	Silvia Adriana Silvestrini – CPO	
Aprovado por: **Approved by:**	Cleber Candido Eduardo – CEO	

Versão / Version V2.1		
Data: **Creation Date:**	Aug 14, 2025	**Comentários / Conteúdo revisado** **Comments / Revised Content**
Criado por: **Created by:**	Comitê de Tecnologia Cesla | Cesla Technology Committee	• Inclusão do item: **10.1 - Transferência Internacional de Dados** • Inclusion of item: **10.1 – International Data Transfers**
Revisado por: **Reviewed by:**	Silvia Adriana Silvestrini – CPO	
Aprovado por: **Approved by:**	Cleber Candido Eduardo – CEO	

Versão / Version V2.2		
Data: **Creation Date:**	Aug 22, 2025	**Comentários / Conteúdo revisado** **Comments / Revised Content**
Criado por: **Created by:**	Comitê de Tecnologia Cesla | Cesla Technology Committee	• A versão V2.2 da Política de Privacidade promoveu a revisão integral do documento para adequá-lo à atuação da **Cesla como operadora (Processor)** e dos **clientes como controladores (Controllers)**, em conformidade com a **Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)**. Todas as seções foram revisadas para refletir a segregação de responsabilidades e garantir alinhamento com as obrigações legais, contratuais e regulatórias vigentes. • Version V2.2 of the Privacy Policy carried out a comprehensive review of the document to align it with the role of **Cesla as Processor** and **clients as Controllers**, in compliance with the **Brazilian General Data Protection Law (LGPD – Law No. 13.709/2018)**. All sections were updated to reflect the segregation of responsibilities and ensure alignment with applicable legal, contractual, and regulatory obligations.
Revisado por: **Reviewed by:**	Silvia Adriana Silvestrini – CPO	
Aprovado por: **Approved by:**	Cleber Candido Eduardo – CEO	

Local de Armazenamento do Documento

O arquivo "**Cesla Privacy Policy_Bilingual_V2.2_Aug2025.docx"** está armazenado no repositório oficial da Cesla, com controle de versão e acesso restrito às áreas autorizadas, conforme estrutura a seguir:

📁 **SharePoint > Governança > Documentos > Planos e Políticas > Privacidade > Cesla Privacy Policy_Bilingual_V2.2_Ago2025.docx**

Este diretório é gerenciado pelo Comitê de Tecnologia, e as atualizações do documento são registradas com controle de histórico e revisão. A versão atual está identificada como **V2.2 – August 2025**, com status **Aprovado**.

Document Storage Location

The file "**Cesla Privacy Policy_Bilingual_V2.2_Aug2025.docx"** is stored in Cesla's official repository, with version control and restricted access to authorized departments, according to the following structure:

📁 **SharePoint > Governança > Documentos > Planos e Políticas > Privacidade > Cesla Privacy Policy_Bilingual_V2.2_Aug2025.docx**

This directory is managed by the Technology Committee, and document updates are recorded with version history and revision control. The current version is identified as **V2.2 – August 2025**, with the status **Approved**.

1. Introdução

Em vigor a partir de 22 de Agosto de 2025.

A presente Política de Privacidade tem como finalidade informar de forma clara e transparente como os dados pessoais são tratados no âmbito da plataforma Cesla.

Nos termos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD):

- O cliente contratante da licença da plataforma Cesla é o Controlador dos dados pessoais, responsável por definir as finalidades e os meios do tratamento.
- A Cesla Tecnologia atua como Operadora, processando dados pessoais única e exclusivamente de acordo com as instruções documentadas do cliente controlador, nos limites do contrato firmado e da legislação vigente.

A Cesla poderá, adicionalmente, tratar dados pessoais **estritamente necessários** para a execução do contrato, suporte técnico, segurança da informação, registros de auditoria e cumprimento de obrigações legais próprias. Nesses casos, o tratamento seguirá as bases legais adequadas, sem prejuízo das responsabilidades do cliente como controlador.

Para dúvidas, solicitações ou reclamações relacionadas ao tratamento de dados pessoais, o titular poderá entrar em contato com o Encarregado pelo Tratamento de Dados (DPO) através do e-mail **dpo@intuix.com**.

2. Glossário

Para facilitar sua leitura e compreensão desta Política de Privacidade, segue um resumo das definições de termos usados com recorrência ao longo deste documento:

- **Titular de Dados:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No contexto da Cesla, normalmente é o cliente contratante da licença.
- **Operador:** Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador. A Cesla Tecnologia atua como operadora da Cesla.
- **Suboperadores**: Terceiros contratados pela Cesla para apoiar a execução dos serviços, tais como provedores de infraestrutura e segurança (ex.: Microsoft Azure, EVEO, Cloudflare, Firebase).
- **Dado Pessoal:** Informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, e-mail, endereço IP, entre outros.
- **Dado Pessoal Sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, biometria, entre outros, cuja proteção é reforçada pela LGPD.
- **LGPD (Lei Geral de Proteção de Dados):** Lei nº 13.709/2018, que regula o tratamento de dados pessoais no Brasil, inclusive nos meios digitais.
- **Token de Acesso:** Código criptografado utilizado para autenticar sessões de usuários na plataforma, com validade limitada e renovação controlada.
- **SSO (Single Sign-On):** Mecanismo que permite ao usuário acessar múltiplos sistemas com uma única autenticação centralizada, utilizado via Entra ID e FusionAuth na Cesla.
- **MFA (Autenticação Multifator):** Camada extra de segurança que exige mais de um fator de verificação (como senha + código de verificação) para autenticação.
- **Logs de Auditoria:** Registros automáticos das ações realizadas pelos usuários na plataforma, contendo informações como login, horário, IP, ação executada, entre outros.
- **SIEM (Security Information and Event Management):** Sistema de monitoramento e análise de eventos de segurança, utilizado para detectar e responder a possíveis ameaças e incidentes.
- **Incident Response Plan (IRP):** Documento que define como a Cesla detecta, responde e documenta incidentes de segurança que impactam os dados ou sistemas da plataforma.
- **Business Continuity Plan (BCP):** Estrutura de governança e processos adotados para manter ou restabelecer os serviços essenciais da Cesla diante de falhas críticas ou desastres.
- **EPS (Empresa Prestadora de Serviço):** Organização contratada pelo cliente da Cesla para executar atividades operacionais. Seus dados e documentos são gerenciados em ambiente segregado e com licenciamento próprio.

3. Finalidade

A presente Política tem como finalidade esclarecer de forma transparente como os dados pessoais são tratados no âmbito da plataforma Cesla.

- O cliente contratante (controlador) define as finalidades e os meios do tratamento de dados pessoais realizados na plataforma.
- A Cesla Tecnologia (operadora) executa o tratamento de acordo com as instruções documentadas do cliente controlador, aplicando medidas técnicas e organizacionais adequadas para assegurar a confidencialidade, integridade e disponibilidade dos dados.
- Sempre que necessário, a Cesla poderá realizar tratamento mínimo de dados pessoais estritamente necessários para:
    - Execução do contrato firmado com o cliente;
    - Cumprimento de obrigações legais ou regulatórias próprias;
    - Suporte técnico, manutenção de logs e registros de segurança;
    - Monitoramento e auditoria para fins de integridade da plataforma.

Em todos os cenários, a Cesla mantém a rastreabilidade e segurança das operações, respeitando as instruções do controlador e as disposições da LGPD.

4. Bases Legais

O tratamento de dados pessoais realizado no âmbito da plataforma Cesla observa as bases legais previstas na Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD).

- **Cliente Controlador**: é o responsável por definir e justificar a base legal aplicável a cada tratamento realizado na plataforma (ex.: consentimento, obrigação legal, execução de contrato, legítimo interesse, proteção da vida, entre outros).
- **Cesla Operadora**: executa o tratamento de dados pessoais unicamente conforme instruções documentadas do cliente controlador, nos limites da base legal definida por este.

Além disso, a Cesla poderá adotar bases legais próprias, quando realizar o tratamento estritamente necessário para:

- Cumprimento de obrigações legais ou regulatórias que lhe sejam aplicáveis;
- Execução do contrato firmado com o cliente;
- Proteção da segurança da informação, auditoria e prevenção a incidentes;
- Exercício regular de direitos em processos administrativos, judiciais ou arbitrais.

5. Dados Coletados

A coleta e inserção de dados pessoais na plataforma Cesla é realizada pelos clientes contratantes (controladores) e suas empresas prestadoras de serviço (EPSs), conforme suas finalidades específicas de tratamento.

A Cesla Tecnologia, na qualidade de operadora, processa tais dados exclusivamente de acordo com as instruções documentadas do cliente controlador, aplicando medidas técnicas e organizacionais para garantir segurança, rastreabilidade e conformidade legal.

Os principais grupos de dados que podem ser tratados na plataforma incluem:

- **Dados de Identificação**: Nome completo, e-mail corporativo, CPF, telefone, empresa vinculada, cargo/função e outras informações cadastrais básicas.
- **Dados de Autenticação e Acesso**: Nome de usuário (login), tokens de sessão, autenticação via SSO (Single Sign-On), múltiplos fatores de autenticação (MFA), logs de login e registros de tempo de acesso.
- **Dados de Navegação e Uso da Plataforma**: Endereço IP, datas e horários de acesso, registros de ações realizadas dentro dos módulos, menus acessados e operações executadas.
- **Dados Operacionais**: Informações preenchidas em formulários, permissões atribuídas, uploads de documentos, interações com APIs, respostas a checklists e comentários inseridos na plataforma.

- **Dados Técnicos do Dispositivo e Conexão**: Tipo de dispositivo, navegador utilizado, sistema operacional, resolução de tela e dados de rede/internet utilizados durante a navegação.

A Cesla poderá ainda coletar e tratar dados estritamente necessários para execução contratual, suporte técnico, auditoria e segurança da informação (ex.: registros de logs, trilhas de auditoria e monitoramento de incidentes).

6. Finalidade do Tratamento

Os dados pessoais inseridos na plataforma Cesla são tratados conforme os princípios da necessidade, finalidade, segurança e responsabilização previstos na LGPD.

- O **cliente contratante (controlador)** é o responsável por definir as finalidades e bases legais do tratamento dos dados pessoais.
- A **Cesla Tecnologia (operadora)** executa o processamento exclusivamente em nome do cliente controlador, aplicando controles técnicos e organizacionais que asseguram a confidencialidade, integridade, disponibilidade e rastreabilidade das informações.

As principais finalidades de tratamento que podem ser instruídas pelo controlador e processadas pela Cesla incluem:

- Assegurar o funcionamento técnico da plataforma, incluindo autenticação de usuários, gerenciamento de permissões, controle de sessões e integridade dos dados;
- Garantir a segurança da informação, com aplicação de controles de acesso, registros de atividade, rastreabilidade e resposta a incidentes;
- Apoiar o cumprimento de obrigações legais, contratuais e regulatórias aplicáveis ao cliente controlador (ex.: gestão de terceiros, qualificação de prestadores de serviço, saúde e segurança do trabalho);
- Apoiar a continuidade operacional e os planos de recuperação de desastres, conforme previsto no Plano de Continuidade de Negócios (BCP);
- Monitorar e auditar o uso da plataforma, promovendo a conformidade com normas internas e exigências de clientes;
- Personalizar e aprimorar a experiência do usuário, de acordo com as configurações e permissões definidas pelo cliente controlador.

Além disso, a Cesla poderá realizar tratamento de dados **estritamente necessários** para atender às suas próprias obrigações contratuais, legais ou de segurança (como manutenção de logs técnicos, monitoramento de incidentes e suporte operacional).

6.1. Tratamento de Dados Pessoais Sensíveis

Dependendo do contexto de uso da plataforma e da natureza das informações inseridas, poderão ser tratados dados pessoais sensíveis, tais como: informações de saúde, exames médicos ocupacionais (ASO), certificados de treinamentos, documentos obrigatórios para fins legais, entre outros.

- O cliente contratante (controlador) é responsável por decidir quando e quais dados pessoais sensíveis serão coletados, bem como por garantir a base legal adequada para seu tratamento (ex.: obrigação legal, consentimento, proteção da vida ou saúde, execução de políticas públicas, exercício regular de direitos).
- A Cesla Tecnologia (operadora) processa esses dados única e exclusivamente de acordo com as instruções documentadas do cliente controlador, assegurando que os seguintes requisitos mínimos sejam observados:
    - Finalidade legítima e previamente definida pelo controlador;
    - Restrições de acesso técnico e administrativo, com perfis de acesso atribuídos pelo cliente;
    - Controles de segurança e confidencialidade compatíveis com padrões internacionais (ex.: criptografia, rastreabilidade, segregação de ambientes);
    - Registro e auditoria de todas as operações realizadas.

Em nenhuma hipótese a Cesla utilizará dados pessoais sensíveis para finalidades próprias ou incompatíveis com as instruções do controlador.

7. Compartilhamento de Dados

A Cesla poderá compartilhar dados pessoais tratados na plataforma apenas em duas situações distintas:

1. **Suboperadores contratados diretamente pela Cesla**
   - Para viabilizar a infraestrutura e a segurança da plataforma, a Cesla utiliza provedores de serviços de tecnologia (Microsoft Azure, EVEO, Cloudflare, Firebase).
   - Esses fornecedores atuam como suboperadores da Cesla, vinculados contratualmente à obrigação de:
     - Garantir níveis adequados de segurança da informação e proteção à privacidade;
     - Limitar o uso dos dados exclusivamente à finalidade contratada;
     - Manter confidencialidade, rastreabilidade e conformidade com padrões internacionais, como ISO/IEC 27001.

2. **Terceiros designados pelo cliente contratante (Controlador)**
   - O cliente controlador pode autorizar a integração da plataforma Cesla com sistemas ou parceiros de sua escolha (ex.: controle de acesso, portaria, medicina ocupacional, segurança do trabalho e afins).
   - Nesses casos, a responsabilidade por documentar, justificar e estabelecer contratos com esses terceiros é exclusiva do cliente controlador e de suas EPSs vinculadas.

A Cesla não compartilha dados por iniciativa própria com terceiros externos que não sejam seus suboperadores técnicos. Todo e qualquer compartilhamento além desse escopo dependerá de instrução documentada do cliente controlador.

7.1. Garantia de Segurança e Privacidade no Compartilhamento de Dados

A segurança e a privacidade no compartilhamento de dados seguem a seguinte divisão de responsabilidades:

1. **Responsabilidade do Cliente Controlador**

   - Garantir que os terceiros por ele designados (ex.: sistemas de portaria, medicina ocupacional, segurança do trabalho, fornecedores de integração) estejam em conformidade com a LGPD e demais normas aplicáveis.
   - Formalizar contratos, aditivos ou instrumentos jurídicos necessários com tais terceiros, assegurando cláusulas de confidencialidade, privacidade e segurança.
   - Definir e justificar a base legal aplicável ao compartilhamento.

2. **Responsabilidade da Cesla Operadora**

   - Aplicar controles técnicos e contratuais junto aos suboperadores por ela contratados (Microsoft Azure, EVEO, Cloudflare, Firebase e outros de infraestrutura e segurança).
   - Exigir desses suboperadores compromissos formais quanto a:
     - Confidencialidade das informações tratadas;
     - Uso limitado à finalidade contratada;
     - Implementação de controles técnicos e organizacionais compatíveis com normas internacionais, como ISO/IEC 27001/27035.
   - Realizar, sempre que aplicável, validações técnicas e contratuais para confirmar a aderência desses suboperadores à LGPD e aos padrões de segurança da informação.

A Cesla não assume responsabilidade por integrações realizadas diretamente pelo cliente controlador com terceiros fora do seu escopo contratual.

8. Segurança da Informação

A Cesla Tecnologia, na qualidade de operadora de dados pessoais, adota medidas técnicas e organizacionais rigorosas para proteger as informações tratadas na plataforma, garantindo sua confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade.

Essas medidas são aplicadas em conformidade com as instruções do cliente controlador, com contratos vigentes e com a legislação aplicável (LGPD), abrangendo:

- **Autenticação e Acesso**
  - O controle, gerenciamento, atualização e revogação de acessos de usuários ao sistema é de responsabilidade de cada parte:
    - Cesla em relação aos seus próprios colaboradores e usuários internos;
    - Clientes controladores em relação aos seus usuários cadastrados;
    - EPSs (Empresas Prestadoras de Serviço) em relação aos seus colaboradores cadastrados.
  - **Para usuários da Cesla:** são implementados controles rigorosos de acesso, incluindo login via SSO integrado ao Entra ID, com MFA (autenticação multifator) obrigatório, e perfis de acesso definidos conforme o princípio do privilégio mínimo.
  - **Para usuários de clientes:** o login via SSO corporativo é opcional, porém recomendado para reforço de segurança.
  - **Para usuários de EPSs:** não há opção de login via SSO; o acesso é gerenciado diretamente pelos administradores da licença da EPS.
  - **Para todos os usuários da plataforma**, o uso de MFA é obrigatório, independentemente do modelo de autenticação adotado.

Além disso, a plataforma disponibiliza ao cliente controlador a funcionalidade de cadastro e gestão ilimitada de perfis de acesso, permitindo criar, alterar, ativar ou inativar perfis de forma autônoma. O cliente deve garantir que esses perfis respeitem o princípio do privilégio mínimo, assegurando que cada usuário tenha acesso apenas às funcionalidades necessárias ao desempenho de suas funções.

- **Proteção de Dados**
  - Criptografia em repouso (SHA-512) e em trânsito (TLS 1.2+ com camada adicional de AES-256-CBC).
  - Pseudonimização e segregação de ambientes para dados sensíveis.
- **Controle de Sessões**
  - Sessões autenticadas com tokens expiráveis e rastreáveis.
  - Expiração configurada conforme boas práticas de segurança (1h de duração, com renovação limitada).
- **Monitoramento e Auditoria**
  - Logs de auditoria detalhados mantidos por pelo menos 5 anos.
  - Ferramentas de segurança como SIEM (Security Onion), WAF (Cloudflare), Fail2Ban e monitoramento de erros (Firebase).
- **Segregação de Ambientes**
  - Separação entre ambientes de desenvolvimento, QA, homologação e produção, evitando impactos cruzados.

A Cesla garante que todas as medidas de segurança sejam continuamente monitoradas, testadas e aprimoradas, conforme normas internacionais (ISO/IEC 27001, 27035) e alinhadas aos planos de resposta a incidentes (IRP), continuidade de negócios (BCP) e recuperação de desastres (DRP).

9. Direitos do Usuário (Titular dos Dados)

Em conformidade com a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), os titulares de dados pessoais tratados na plataforma Cesla possuem os seguintes direitos:

- Solicitar a confirmação da existência de tratamento de seus dados;
- Ter acesso aos dados armazenados e receber informações claras sobre sua finalidade;
- Requisitar a correção de dados incompletos, inexatos ou desatualizados;
- Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos;
- Obter informações sobre compartilhamentos realizados com terceiros;
- Requerer a portabilidade dos dados, observados os segredos comercial e industrial;
- Revogar consentimentos fornecidos, quando aplicável;
- Manifestar oposição ao tratamento realizado com base em legítimo interesse, quando couber.

Responsabilidades

- O cliente contratante (controlador) é o responsável por receber, avaliar e responder às solicitações dos titulares, conforme as bases legais que justificam o tratamento.

- A Cesla Tecnologia (operadora) presta apoio técnico e administrativo ao controlador, garantindo que os dados estejam acessíveis, íntegros e rastreáveis para atendimento das solicitações.

Como exercer os direitos

Os titulares devem encaminhar suas solicitações prioritariamente ao cliente controlador responsável pelo ambiente em que seus dados foram inseridos.

Nos casos em que a solicitação for recebida diretamente pela Cesla, esta será analisada e redirecionada ao controlador aplicável, mantendo o suporte necessário para que o pedido seja atendido em conformidade com a LGPD.

10. Armazenamento e Retenção

Os dados pessoais tratados na plataforma Cesla são armazenados em ambiente de nuvem segura, utilizando provedores certificados (Microsoft Azure e EVEO) e suboperadores contratados pela Cesla para fins de infraestrutura e segurança.

- O **cliente contratante (controlador)** é responsável por definir, em contrato, as políticas de retenção aplicáveis aos dados pessoais de seus colaboradores, prestadores de serviço (EPSs) e demais titulares.
- A **Cesla Tecnologia (operadora)** garante que os dados sejam mantidos de forma segura, com aplicação de criptografia, segregação de ambientes e logs de auditoria, cumprindo sempre as instruções recebidas do cliente controlador.

Prazos de retenção aplicados pela plataforma Cesla

- **Dados vinculados à conta do cliente controlador** (administradores, operadores, responsáveis técnicos): armazenados por até 60 dias após a rescisão contratual (ou conforme cláusula contratual específica) e, após este prazo, são definitivamente excluídos da plataforma. Durante o período de 60 dias, todos os dados estarão disponíveis para que o cliente retire uma cópia, seguindo critérios e mecanismos de transferência segura.
- **Dados de EPSs e colaboradores cadastrados pelo cliente** (ex.: informações pessoais, certificados de treinamento, ASOs, documentos de qualificação):
    - São mantidos por até 20 anos, desde que o contrato do cliente controlador esteja ativo, para fins legais, regulatórios e trabalhistas.
    - Em caso de rescisão contratual com o cliente controlador, os dados poderão ser disponibilizados ao cliente dentro do prazo de 60 dias (ou conforme cláusula contratual específica). Após este prazo, serão definitivamente excluídos da base da Cesla.
    - Caso a EPS e seus colaboradores estejam vinculados a outro cliente ativo, os dados permanecerão na base da Cesla, vinculados ao contrato do novo cliente controlador, garantindo a continuidade do tratamento conforme as bases legais aplicáveis.
    - O acesso da EPS à plataforma será mantido enquanto existir relação comercial ativa com algum cliente. Após o encerramento da prestação de serviço, o acesso permanecerá ativo por 365 dias e, após este prazo, a licença da EPS será inativada. Os dados, contudo, permanecerão armazenados para fins de controle, auditoria e obrigações legais do cliente controlador.
    - A EPS poderá solicitar, a qualquer momento, acesso às informações armazenadas, mediante validação do cliente controlador.
- **Logs de login, trilhas de auditoria e registros de rastreabilidade**: armazenados pela Cesla por, no mínimo, 5 anos, inclusive após a rescisão contratual, exclusivamente para fins de segurança da informação, auditoria, conformidade regulatória e exercício regular de direitos. Após esse período, os registros são eliminados de forma segura.

A Cesla somente manterá dados além desses períodos mediante instrução documentada do cliente controlador ou em cumprimento de obrigações legais próprias.

10.1. Transferência Internacional de Dados

A Cesla poderá realizar transferência internacional de dados pessoais quando necessário para a operação da plataforma, em conformidade com a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) e demais legislações aplicáveis.

- O **cliente contratante (controlador)** é responsável por autorizar e definir a base legal aplicável ao tratamento que envolva transferência internacional de dados.
- A **Cesla Tecnologia (operadora)** executa tais transferências exclusivamente no âmbito da operação da plataforma, utilizando suboperadores certificados de infraestrutura e segurança.

Cenários de transferência internacional atualmente aplicáveis:

- **Armazenamento de backups**: parte dos backups da plataforma Cesla é armazenada em datacenters da Microsoft Azure localizados nos Estados Unidos (região Central US), com proteção conforme padrões internacionais, incluindo criptografia AES-256-CBC em trânsito, SHA-512 em repouso e certificação ISO/IEC 27001:2022.
- **Armazenamento de documentos e imagens**: arquivos enviados e processados pela plataforma (imagens, evidências e documentos) podem ser armazenados no Cloudflare R2, em servidores distribuídos globalmente, assegurando que a transferência siga medidas técnicas e organizacionais adequadas.

Condições de retenção aplicáveis às transferências:

- **Dados vinculados ao cliente controlador**: após a rescisão contratual, permanecem disponíveis por até 60 dias para cópia pelo cliente, sendo definitivamente excluídos após esse prazo.
- **Dados de EPSs e colaboradores**: podem ser mantidos por até 20 anos enquanto houver contrato ativo do cliente controlador, para fins legais e regulatórios. Em caso de rescisão, podem ser exportados para o cliente dentro de 60 dias, sendo depois excluídos da base da Cesla, exceto se vinculados a outro cliente ativo.
- **Logs de login, trilhas de auditoria e registros de rastreabilidade**: armazenados por pelo menos 5 anos, inclusive após a rescisão contratual, exclusivamente para fins de segurança da informação, auditoria, conformidade regulatória e exercício regular de direitos.

Todos os suboperadores contratados pela Cesla (Azure, EVEO, Cloudflare, Firebase) são obrigados contratualmente a:

- Adotar cláusulas contratuais padrão e certificações internacionais (ex.: ISO/IEC 27001);
- Garantir controles técnicos e organizacionais compatíveis com a LGPD;
- Cumprir obrigações de confidencialidade, rastreabilidade e limitação de uso.

Sempre que aplicável, a Cesla aplica medidas adicionais, como pseudonimização e controle estrito de acesso, para mitigar riscos relacionados à transferência internacional de dados.

11. Responsabilidades do Cliente Contratante e das Empresas Prestadoras de Serviço (EPSs)

A Cesla Tecnologia, como operadora, realiza o tratamento de dados pessoais exclusivamente conforme instruções documentadas do cliente contratante (controlador), nos limites do contrato firmado.

São de responsabilidade exclusiva do cliente controlador e de suas EPSs vinculadas:

- Garantir que exista base legal válida para o tratamento dos dados pessoais inseridos na plataforma Cesla, incluindo consentimentos quando aplicável;
- Informar seus colaboradores, prestadores e demais titulares sobre o tratamento de seus dados pessoais na plataforma, inclusive quanto à possibilidade de armazenamento em nuvem e transferências internacionais realizadas por suboperadores da Cesla;
- Formalizar cláusulas contratuais apropriadas reconhecendo que os dados pessoais e documentos enviados poderão ser utilizados para fins de qualificação, rastreabilidade, auditoria e segurança operacional, conforme obrigações legais e contratuais;
- Solicitar, dentro do prazo de 60 dias após a rescisão contratual, a extração de cópia dos dados armazenados, garantindo que os titulares sejam informados sobre a exclusão definitiva dos dados após esse período;
- Documentar e justificar integrações com sistemas e fornecedores externos que não sejam suboperadores da Cesla.

A Cesla **não se responsabiliza** pela ausência de formalização adequada entre o cliente controlador, suas EPSs e os colaboradores cadastrados. Qualquer reivindicação de titulares de dados deve ser inicialmente direcionada ao cliente controlador, que é o responsável legal pelas decisões de tratamento.

A Cesla mantém a obrigação de:

- Assegurar retenção de dados de EPSs e colaboradores por até 20 anos, exclusivamente quando houver contrato ativo do cliente controlador ou vinculação a outro cliente ativo;
- Manter logs de login, auditoria e rastreabilidade por, no mínimo, 5 anos, inclusive após rescisão contratual, para fins de segurança, conformidade regulatória e exercício regular de direitos;
- Aplicar controles técnicos e organizacionais que assegurem a confidencialidade, integridade e disponibilidade dos dados tratados;
- Apoiar o cliente controlador no atendimento às solicitações dos titulares, conforme previsto na LGPD.

12. Comunicação de Incidentes e Não Conformidades

Todos os usuários da plataforma Cesla — incluindo clientes contratantes, empresas prestadoras de serviço (EPSs) e colaboradores da Cesla Tecnologia — devem adotar postura ativa na identificação e comunicação de situações que possam representar risco à segurança da informação ou à conformidade com a LGPD.

Em caso de identificação ou suspeita de:

- Vazamento ou acesso indevido a dados pessoais;
- Comportamento anômalo no sistema ou falhas técnicas relevantes;
- Compartilhamento não autorizado de dados;
- Utilização indevida de credenciais ou permissões de acesso;
- Não conformidade contratual ou legal relacionada ao tratamento de dados;
- Falhas de segurança em autenticação, permissões ou integridade das informações;
- Descumprimento da LGPD ou de cláusulas contratuais;

O incidente deve ser comunicado **imediatamente** à equipe Cesla por meio dos canais institucionais de suporte ou ao Encarregado de Dados (DPO), via **dpo@intuix.com**.

Responsabilidades

- **Cesla (operadora):**
    - Atua tecnicamente na detecção, contenção, análise e registro do incidente;
    - Fornece evidências e relatórios técnicos ao cliente controlador, inclusive com base em logs de auditoria e rastreabilidade retidos por no mínimo 5 anos, mesmo após eventual rescisão contratual;
    - Apoia na execução do Plano de Resposta a Incidentes (IRP), garantindo rastreabilidade e documentação.

- **Cliente contratante (controlador):**
    - É o responsável por avaliar o impacto do incidente sobre os titulares;
    - Decide sobre a necessidade de comunicação oficial aos titulares afetados e à ANPD (Autoridade Nacional de Proteção de Dados), conforme previsto na LGPD;
    - Conduz as medidas de comunicação externas (titulares, reguladores, parceiros), com suporte técnico da Cesla quando aplicável.

É expressamente vedado o uso, compartilhamento ou armazenamento de dados acessados indevidamente. Qualquer violação poderá resultar em responsabilização civil, penal e contratual, conforme a legislação vigente e os compromissos assumidos com os titulares.

13. Propriedade Intelectual

Todos os direitos de propriedade intelectual relacionados à **plataforma Cesla** — incluindo seus módulos, funcionalidades, interface, estruturas de dados, fluxos operacionais, marca, identidade visual, código-fonte, bancos de dados e demais componentes técnicos — são de titularidade exclusiva da **Cesla Tecnologia**.

É expressamente vedado a qualquer usuário, cliente controlador, EPS ou terceiro:

- Reproduzir, copiar, modificar, descompilar, realizar engenharia reversa ou criar obras derivadas com base em qualquer módulo ou funcionalidade da plataforma Cesla;
- Utilizar a plataforma para finalidades não autorizadas contratualmente ou fora do escopo da licença concedida;
- Transferir, ceder ou sublicenciar o uso da plataforma sem autorização formal da Cesla Tecnologia.

A contratação da licença de uso da plataforma concede ao cliente controlador um direito de uso não exclusivo, intransferível e limitado ao período contratual, conforme definido no contrato comercial.

O uso indevido poderá gerar responsabilização civil, penal e administrativa, além das sanções previstas contratualmente e na legislação vigente.

Este item não afeta os direitos do cliente controlador sobre os dados pessoais e operacionais inseridos na plataforma, os quais permanecem sob sua titularidade e responsabilidade legal, nos termos da LGPD.

14. Encarregado pelo Tratamento de Dados (DPO)

A Cesla Tecnologia designou um Encarregado pelo Tratamento de Dados (Data Protection Officer – DPO), responsável por atuar como canal de comunicação entre a Cesla, os clientes controladores, os titulares de dados, a Autoridade Nacional de Proteção de Dados (ANPD) e demais partes interessadas.

Responsabilidades do DPO da Cesla

- Atuar como ponto de contato de suporte ao cliente controlador, fornecendo orientações técnicas e administrativas sobre privacidade e segurança de dados;
- Apoiar os clientes no atendimento de solicitações dos titulares, quando recebidas pela Cesla, garantindo que sejam devidamente encaminhadas ao controlador responsável;
- Manter registros de incidentes e comunicações relacionadas ao tratamento de dados, assegurando rastreabilidade e conformidade;
- Orientar colaboradores internos e suboperadores da Cesla sobre práticas de proteção de dados pessoais;
- Monitorar a aderência da Cesla às instruções contratuais e à LGPD, atuando em alinhamento com os controladores.

Comunicação com titulares de dados

- O **cliente contratante (controlador)** é o responsável principal por responder às solicitações dos titulares de dados (ex.: acesso, correção, exclusão, oposição).
- Caso a Cesla receba diretamente uma solicitação de titular, esta será registrada e encaminhada ao cliente controlador, com o devido suporte técnico para que o pedido seja tratado dentro dos prazos legais.

Para entrar em contato com o DPO da Cesla Tecnologia, utilize o canal oficial: **dpo@intuix.com**

15. Atualizações e Revisões

A presente Política de Privacidade será revisada periodicamente, com frequência mínima anual, ou sempre que ocorrerem:

- Alterações significativas na legislação aplicável, especialmente relacionadas à proteção de dados pessoais;
- Atualizações nos serviços, funcionalidades ou módulos da plataforma Cesla que impactem o tratamento de dados;
- Mudanças relevantes nos processos internos de segurança da informação, privacidade ou governança de dados.

Responsabilidades na atualização

- A **Cesla Tecnologia (operadora)** é responsável por manter esta Política alinhada às normas de segurança, boas práticas e contratos vigentes, comunicando formalmente os clientes controladores sobre alterações relevantes.
- O **cliente controlador** é responsável por avaliar e, quando necessário, informar os titulares de dados sob sua responsabilidade sobre eventuais mudanças que impactem seus direitos.

Todas as versões da Política possuem controle de histórico e versionamento. A versão mais atual estará sempre disponível nos canais oficiais da Cesla, em repositório seguro.

16. Confidencialidade

Todas as informações e dados pessoais tratados na plataforma Cesla são considerados **confidenciais** e protegidos contra acesso, uso ou divulgação não autorizada.

Responsabilidades da Cesla (operadora)

- Adotar medidas técnicas e administrativas rigorosas para preservar a confidencialidade dos dados processados em nome do cliente controlador;
- Exigir cláusulas de confidencialidade e segurança de seus colaboradores e suboperadores (ex.: Azure, EVEO, Cloudflare, Firebase);
- Garantir rastreabilidade por meio de logs de auditoria e monitoramento contínuo das operações realizadas.

Responsabilidades do Cliente (controlador)

- Garantir que os dados inseridos na plataforma sejam tratados em conformidade com a LGPD e utilizados apenas para as finalidades legítimas definidas contratualmente;
- Assegurar que seus próprios colaboradores, EPSs e parceiros mantenham a confidencialidade dos dados sob sua responsabilidade;
- Comunicar a Cesla sempre que identificar violações ou riscos de quebra de confidencialidade relacionados ao uso da plataforma.

Restrições

É vedado a qualquer usuário, colaborador ou terceiro:

- Compartilhar ou utilizar dados acessados de forma indevida;
- Divulgar informações tratadas na plataforma sem autorização do cliente controlador;
- Reutilizar informações para fins pessoais, comerciais ou não autorizados.

A violação das obrigações de confidencialidade poderá resultar em **sanções administrativas, civis ou criminais**, conforme previsto na LGPD, na legislação aplicável e nos contratos firmados entre as partes.

17. Disposições Finais

A presente Política de Privacidade tem como objetivo garantir transparência, segurança e conformidade no tratamento de dados pessoais realizado na plataforma Cesla.

- O cliente contratante (controlador) é o responsável principal pelas decisões relativas ao tratamento dos dados pessoais, incluindo definição de finalidades, bases legais, prazos de retenção e comunicação com os titulares.
- A Cesla Tecnologia (operadora) atua exclusivamente sob instruções documentadas do cliente controlador, aplicando medidas técnicas e organizacionais adequadas para proteger os dados, apoiar no atendimento aos direitos dos titulares e manter a rastreabilidade das operações.
- Os prazos de retenção aplicados pela plataforma seguem critérios definidos contratualmente e legalmente:
    - 60 dias para disponibilização dos dados após a rescisão contratual, antes da exclusão definitiva;
    - Até 20 anos para dados de EPSs e colaboradores, quando vinculados a clientes ativos ou conforme obrigações legais e trabalhistas;
    - 5 anos para logs de login, trilhas de auditoria e registros de rastreabilidade, inclusive após rescisão contratual, exclusivamente para fins de segurança, conformidade regulatória e exercício regular de direitos.
- As transferências internacionais de dados são realizadas unicamente no contexto operacional da Cesla como operadora, utilizando suboperadores certificados (Azure, EVEO, Cloudflare, Firebase), sempre em conformidade com as instruções do controlador e com as exigências da LGPD.

A Cesla compromete-se a manter esta Política atualizada em conformidade com a legislação, normas internacionais de segurança da informação (ISO/IEC 27001, 27035) e contratos estabelecidos com seus clientes.

18. Revisão e Aprovação

Esta Política de Privacidade foi revisada e aprovada conforme os processos internos de governança da Cesla Tecnologia.

A revisão periódica garante que o documento permaneça atualizado em relação à LGPD, às normas internacionais de segurança da informação (ex.: ISO/IEC 27001, 27035) e aos contratos firmados com os clientes.

A validação deste documento não altera a natureza das responsabilidades:

- O **cliente contratante** permanece como **controlador** dos dados pessoais inseridos na plataforma;
- A **Cesla Tecnologia** atua como **operadora**, executando o tratamento conforme instruções documentadas do cliente.

Responsáveis

Revisão Técnica:

- **Silvia Adriana Silvestrini** — *Chief Product Officer (CPO)*
  - Responsável técnica principal.

Aprovação Executiva:

- **Cleber Candido Eduardo** — *Chief Executive Officer (CEO)*
  - Responsável institucional.

Campinas/SP, 22 de agosto de 2025.

ENGLISH VERSION – OFFICIAL TRANSLATION

1. Introduction

Effective as of August 22, 2025.

This Privacy Policy aims to clearly and transparently explain how personal data is processed within the Cesla platform.

Under the Brazilian General Data Protection Law (Law No. 13.709/2018 – LGPD):

- The client contracting the Cesla platform license is the Controller of personal data, responsible for defining the purposes and means of processing.
- Cesla Tecnologia acts as a Processor, handling personal data solely and exclusively in accordance with the documented instructions of the client (Controller), within the limits of the executed contract and applicable law.

Cesla may additionally process strictly necessary personal data for contract execution, technical support, information security, audit logging, and compliance with its own legal obligations. In such cases, processing will follow the appropriate legal bases, without affecting the client's primary responsibilities as Controller.

For questions, requests, or complaints related to the processing of personal data, the data subject may contact the Data Protection Officer (DPO) via the email dpo@intuix.com .

2. Glossary

To facilitate your reading and understanding of this Privacy Policy, below is a summary of definitions of terms frequently used throughout this document:

- **Data Owner:** A natural person to whom the personal data that is the object of processing refers.
- **Controller:** A natural or legal person, whether governed by public or private law, who is responsible for decisions regarding the processing of personal data. In the context of Cesla, this is usually the client contracting the license.
- **Data Operator:** A natural or legal person who processes personal data on behalf of the controller. Cesla Tecnologia acts as the processor of Cesla.
- **Sub-processors**: Third parties engaged by Cesla to support service delivery, such as infrastructure and security providers (e.g., Microsoft Azure, EVEO, Cloudflare, Firebase).
- **Personal Data:** Information relating to an identified or identifiable natural person, such as name, taxpayer ID (CPF), email, IP address, among others.
- **Sensitive Personal Data:** Personal data about racial or ethnic origin, religious belief, political opinion, health, sex life, biometrics, among others, whose protection is reinforced by the LGPD.
- **GDPL (General Data Protection Law):** Law No. 13.709/2018, which regulates the processing of personal data in Brazil, including in digital media.
- **Access Token:** An encrypted code used to authenticate user sessions on the platform, with limited validity and controlled renewal.
- **SSO (Single Sign-On):** A mechanism that allows the user to access multiple systems with a single centralized authentication, used via Entra ID and FusionAuth in Cesla.
- **MFA (Multi-Factor Authentication):** An additional security layer requiring more than one verification factor (such as password + verification code) for authentication.
- **Audit Logs:** Automatic records of actions performed by users on the platform, containing information such as login, timestamp, IP address, executed action, among others.
- **SIEM (Security Information and Event Management):** A system for monitoring and analyzing security events, used to detect and respond to possible threats and incidents.
- **Incident Response Plan (IRP):** A document defining how Cesla detects, responds to, and documents security incidents that impact data or platform systems.
- **Business Continuity Plan (BCP):** A governance structure and processes adopted to maintain or restore Cesla's essential services in the event of critical failures or disasters.

- **Contractor – Service Provider Company (EPS):** An organization contracted by Cesla's client to perform operational activities. Its data and documents are managed in a segregated environment under its own licensing.

3. Purpose

This Policy aims to transparently clarify how personal data is processed within the Cesla platform.

- The **contracting client (Controller)** defines the purposes and means of personal data processing performed within the platform.
- **Cesla Tecnologia (Processor)** carries out processing in accordance with the Controller's documented instructions, applying appropriate technical and organizational measures to ensure data confidentiality, integrity, and availability.
- Whenever necessary, Cesla may perform minimal processing of strictly necessary personal data for:
    - Execution of the contract with the client;
    - Compliance with its own legal or regulatory obligations;
    - Technical support, maintenance of logs, and security records;
    - Monitoring and auditing to preserve the platform's integrity.

In all scenarios, Cesla ensures traceability and security of operations, respecting the Controller's instructions and the provisions of the LGPD.

4. Legal Bases

The processing of personal data within the Cesla platform complies with the legal bases established by the Brazilian General Data Protection Law (Law No. 13.709/2018 – LGPD).

- **Client Controller**: is responsible for defining and justifying the legal basis applicable to each processing activity performed in the platform (e.g., consent, legal obligation, contract execution, legitimate interest, protection of life, among others).
- **Cesla as Processor**: carries out personal data processing solely in accordance with the Controller's documented instructions, within the limits of the legal basis defined by the Controller.

Additionally, Cesla may rely on its own legal bases when performing strictly necessary processing for:

- Compliance with legal or regulatory obligations applicable to Cesla;
- Execution of the contract signed with the client;
- Information security protection, auditing, and incident prevention;
- Regular exercise of rights in administrative, judicial, or arbitral proceedings.

5. Data Collected

The collection and entry of personal data into the Cesla platform are carried out by contracting clients (Controllers) and their Service Provider Companies (EPSs), in accordance with their specific processing purposes.

Cesla Tecnologia, as the **Processor,** handles such data exclusively in line with the Controller's documented instructions, applying technical and organizational measures to ensure security, traceability, and legal compliance.

The main groups of data that may be processed within the platform include:

- **Identification Data**: Full name, corporate email, taxpayer ID (CPF), phone number, associated company, position/function, and other basic registration information.
- **Authentication and Access Data**: Username (login), session tokens, authentication via SSO (Single Sign-On), multi-factor authentication (MFA), login logs, and access time records.
- **Browsing and Platform Usage Data**: IP address, dates and times of access, records of actions performed within modules, menus accessed, and operations executed.
- **Operational Data**: Information entered in forms, assigned permissions, document uploads, interactions with APIs, checklist responses, and comments added to the platform.

- **Device and Connection Technical Data**: Device type, browser used, operating system, screen resolution, and network/internet data used during navigation.

Cesla may also collect and process strictly necessary data for contract execution, technical support, auditing, and information security (e.g., log records, audit trails, and incident monitoring).

6. Purpose of Processing

Personal data entered into the Cesla platform is processed in accordance with the LGPD principles of necessity, purpose, security, and accountability.

- The **contracting client (Controller)** is responsible for defining the purposes and legal bases for the processing of personal data.
- **Cesla Tecnologia (Processor)** carries out processing solely on behalf of the Controller, applying technical and organizational controls to ensure confidentiality, integrity, availability, and traceability of information.

The main processing purposes that may be instructed by the Controller and executed by Cesla include:

- Ensuring the technical operation of the platform, including user authentication, permission management, session control, and data integrity;
- Guaranteeing information security through access controls, activity logging, traceability, and incident response;
- Supporting compliance with legal, contractual, and regulatory obligations applicable to the Controller (e.g., third-party management, qualification of service providers, occupational health and safety);
- Supporting business continuity and disaster recovery plans, as defined in the Business Continuity Plan (BCP);
- Monitoring and auditing platform usage, promoting compliance with internal standards and client requirements;
- Personalizing and improving the user experience, in accordance with the settings and permissions defined by the Controller.

Additionally, Cesla may process strictly necessary data to comply with its own contractual, legal, or security obligations (such as maintaining technical logs, monitoring incidents, and providing operational support).

6.1. Processing of Sensitive Personal Data

Depending on the context of platform use and the nature of the information entered, sensitive personal data may be processed, such as: health information, occupational medical exams (ASO), training certificates, documents required for legal purposes, among others.

- The **contracting client (Controller)** is responsible for deciding when and which sensitive personal data will be collected, as well as ensuring the appropriate legal basis for its processing (e.g., legal obligation, consent, protection of life or health, execution of public policies, regular exercise of rights).
- **Cesla Tecnologia (Processor)** handles such data solely and exclusively in accordance with the Controller's documented instructions, ensuring that the following minimum requirements are observed:
    - A legitimate and previously defined purpose established by the Controller;
    - Technical and administrative access restrictions, with access profiles assigned by the client;
    - Security and confidentiality controls aligned with international standards (e.g., encryption, traceability, environment segregation);
    - Logging and auditing of all processing operations.

Under no circumstances will Cesla use sensitive personal data for its own purposes or in a manner inconsistent with the Controller's instructions.

7. Data Sharing

Cesla may share personal data processed within the platform only under two distinct circumstances:

1. **Sub-processors directly contracted by Cesla**

- To enable platform infrastructure and security, Cesla relies on technology service providers (Microsoft Azure, EVEO, Cloudflare, Firebase).
- These providers act as sub-processors of Cesla and are contractually bound to:
  - Ensure adequate levels of information security and privacy protection;
  - Use data strictly for the contracted purpose;
  - Maintain confidentiality, traceability, and compliance with international standards such as ISO/IEC 27001.

2. **Third parties designated by the contracting client (Controller)**
   - The Controller may authorize integration of the Cesla platform with systems or partners of its choice (e.g., access control, reception, occupational health, occupational safety, etc.).
   - In such cases, the responsibility for documenting, justifying, and establishing contracts with these third parties lies exclusively with the Controller and its associated EPSs.

Cesla does not independently share data with external third parties other than its technical sub-processors. Any additional sharing beyond this scope will depend on the documented instruction of the Controller.

7.1. Guarantee of Security and Privacy in Data Sharing

Security and privacy in data sharing follow the following division of responsibilities:

1. **Responsibility of the Client Controller**
   - Ensure that third parties designated by the Controller (e.g., access control systems, occupational health, occupational safety, integration providers) comply with the LGPD and other applicable regulations.
   - Formalize contracts, amendments, or other legal instruments with such third parties, ensuring confidentiality, privacy, and security clauses.
   - Define and justify the legal basis applicable to the sharing.

2. **Responsibility of Cesla as Processor**
   - Apply technical and contractual controls with its **sub-processors** (Microsoft Azure, EVEO, Cloudflare, Firebase, and other infrastructure/security providers).
   - Require these sub-processors to formally commit to:
     - Confidentiality of the information processed;
     - Use limited to the contracted purpose;
     - Implementation of technical and organizational controls aligned with international standards, such as ISO/IEC 27001/27035.
   - Conduct, whenever applicable, technical and contractual validations to confirm compliance of these sub-processors with the LGPD and information security standards.

Cesla does not assume responsibility for integrations carried out directly by the Controller with third parties outside Cesla's contractual scope.

8. Information Security

Cesla Tecnologia, as the Processor of personal data, adopts strict technical and organizational measures to protect the information processed within the platform, ensuring its confidentiality, integrity, availability, authenticity, and traceability.

These measures are applied in compliance with the client Controller's instructions, current contracts, and applicable law (LGPD), and include:

- **Authentication and Access**
  - The control, management, updating, and revocation of user access to the system is the responsibility of each party:
    - **Cesla**, for its own employees and internal users;
    - **Client Controllers**, for their registered users;
    - **Service Provider Companies (EPSs)**, for their registered employees.

- **For Cesla users**: strict access controls are enforced, including login via SSO integrated with Entra ID, with mandatory MFA (Multi-Factor Authentication), and access profiles defined in accordance with the principle of least privilege.
- **For Client users**: login via corporate SSO is optional but recommended for enhanced security.
- **For EPS users**: there is no option for SSO login; access is managed directly by the EPS license administrators.
- **For all platform users**, MFA is mandatory, regardless of the authentication model adopted.

In addition, the platform provides the client Controller with the ability to register and manage unlimited access profiles, allowing the creation, modification, activation, or deactivation of profiles autonomously. The client must ensure that these profiles comply with the principle of least privilege, ensuring that each user has access only to the functionalities necessary to perform their duties.

- **Data Protection**
  - Encryption at rest (SHA-512) and in transit (TLS 1.2+ with an additional AES-256-CBC layer).
  - Pseudonymization and environment segregation for sensitive data.
- **Session Control**
  - Authenticated sessions with expirable and traceable tokens.
  - Expiration configured according to security best practices (1h duration, with limited renewal).
- **Monitoring and Auditing**
  - Detailed audit logs retained for at least 5 years.
  - Security tools such as SIEM (Security Onion), WAF (Cloudflare), Fail2Ban and error monitoring (Firebase).
- **Environment Segregation**
  - Separation between development, QA, staging, and production environments to avoid cross-impact.

Cesla ensures that all security measures are continuously monitored, tested, and improved, in accordance with international standards (ISO/IEC 27001, 27035) and aligned with its Incident Response Plan (IRP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP).

9. User Rights (Data Subject Rights)

In accordance with the Brazilian General Data Protection Law (LGPD – Law No. 13.709/2018), data subjects whose personal data are processed within the Cesla platform have the following rights:

- Request confirmation of the existence of data processing;
- Access the stored data and receive clear information about its purpose;
- Request the correction of incomplete, inaccurate, or outdated data;
- Request the anonymization, blocking, or deletion of unnecessary or excessive data;
- Obtain information about sharing with third parties;
- Request data portability, subject to trade and industrial secrecy;
- Withdraw previously provided consent, when applicable;
- Object to processing carried out on the basis of legitimate interest, when applicable.

Responsibilities

- The **contracting client (Controller)** is responsible for receiving, assessing, and responding to data subject requests, according to the legal bases that justify the processing.
- **Cesla Tecnologia (Processor)** provides technical and administrative support to the Controller, ensuring that data remains accessible, accurate, and traceable for the fulfillment of requests.

How to exercise rights

Data subjects must submit their requests primarily to the client Controller responsible for the environment where their data was entered.

If a request is received directly by Cesla, it will be reviewed and redirected to the applicable Controller, with Cesla providing the necessary support to ensure compliance with the LGPD.

10. Storage and Retention

Personal data processed within the Cesla platform is stored in a secure cloud environment, using certified providers (Microsoft Azure and EVEO) and sub-processors contracted by Cesla for infrastructure and security purposes.

- The **contracting client (Controller)** is responsible for defining, in the agreement, the retention policies applicable to the personal data of its employees, service providers (EPSs), and other data subjects.
- **Cesla Tecnologia (Processor)** ensures that data is securely maintained, applying encryption, environment segregation, and audit logs, always in accordance with the Controller's instructions.

Retention periods applied by the Cesla platform

- **Data linked to the Controller client's account** (administrators, operators, technical managers): retained for up to 60 days after contract termination (or according to a specific contractual clause) and, after this period, are **permanently deleted from the platform**. During the 60-day period, all data will be made available for the client to extract a copy, following applicable criteria and mechanisms for secure transfer.
- **Data of EPSs and their employees registered by the client** (e.g., personal information, training certificates, occupational health certificates, qualification documents):
    - Retained for up to 20 years, provided that the client Controller's contract remains active, for legal, regulatory, and labor purposes.
    - In the event of contract termination with the Controller, data may be made available to the client within 60 days (or according to a specific contractual clause). After this period, the data will be permanently deleted from Cesla's systems.
    - If the EPS and its employees are linked to another active client, the data will remain in Cesla's database, associated with the new Controller client, ensuring continuity of processing based on applicable legal grounds.
    - EPS access to the platform will be maintained while there is an active commercial relationship with at least one client. After service termination, access will remain active for 365 days and, after this period, the EPS license will be deactivated. The data, however, will remain stored for compliance, audit, and legal purposes of the Controller client.
    - The EPS may request access to stored information at any time, subject to validation by the Controller client.
- **Login records, audit trails, and traceability logs**: stored by Cesla for at least 5 years, including after contract termination, exclusively for information security, auditing, regulatory compliance, and the regular exercise of rights. After this period, records are securely deleted.

Cesla will only retain data beyond these periods upon the Controller's documented instruction or to comply with its own legal obligations.

10.1. International Data Transfers

Cesla may carry out international transfers of personal data when necessary for the operation of the platform, in compliance with the Brazilian General Data Protection Law (LGPD – Law No. 13.709/2018) and other applicable legislation.

- The **contracting client (Controller)** is responsible for authorizing and defining the legal basis for any processing involving international data transfers.
- **Cesla Tecnologia (Processor)** performs such transfers solely within the scope of platform operation, using certified infrastructure and security sub-processors.

Current scenarios of international transfer:

- **Backup storage**: part of the Cesla platform backups is stored in Microsoft Azure datacenters located in the United States (Central US region), protected according to international standards, including AES-256-CBC encryption in transit, SHA-512 encryption at rest, and certified under ISO/IEC 27001:2022.
- **Document and image storage**: files uploaded and processed on the platform (images, evidence, and documents) may be stored in Cloudflare R2, on globally distributed servers, ensuring that transfers follow adequate technical and organizational measures.

Retention conditions applicable to transfers:

- **Data linked to the Controller client**: after contract termination, data remains available for up to 60 days for client extraction, and is permanently deleted after this period.
- **Data of EPSs and their employees**: may be retained for up to 20 years while the Controller client's contract remains active, for legal and regulatory purposes. In case of termination, such data may be exported to the client within 60 days, after which it is permanently deleted from Cesla's systems, unless still linked to another active client.
- **Login records, audit trails, and traceability logs**: stored for at least 5 years, including after contract termination, exclusively for information security, auditing, regulatory compliance, and the regular exercise of rights.

All sub-processors engaged by Cesla (Azure, EVEO, Cloudflare, Firebase) are contractually required to:

- Adopt standard contractual clauses and international certifications (e.g., ISO/IEC 27001);
- Ensure technical and organizational controls compliant with LGPD;
- Fulfill obligations of confidentiality, traceability, and purpose limitation.

Whenever applicable, Cesla applies additional measures, such as pseudonymization and strict access control, to mitigate risks related to international data transfers.

11. Responsibilities of the Contracting Client and Service Provider Companies (EPSs)

Cesla Tecnologia, as the Processor, processes personal data exclusively in accordance with the contracting client's (Controller's) documented instructions, within the scope of the executed contract.

The Controller client and its associated EPSs are solely responsible for:

- Ensuring that a valid legal basis exists for processing personal data entered into the Cesla platform, including obtaining consent when applicable;
- Informing their employees, contractors, and other data subjects about the processing of their personal data within the platform, including the possibility of cloud storage and international transfers carried out by Cesla's sub-processors;
- Formalizing appropriate contractual clauses acknowledging that personal data and documents submitted may be used for qualification, traceability, auditing, and operational safety, in accordance with legal and contractual obligations;
- Requesting, within 60 days after contract termination, the extraction of a copy of stored data, ensuring that data subjects are informed about the permanent deletion of data after this period;
- Documenting and justifying integrations with external systems and providers that are not Cesla's sub-processors.

Cesla **is not responsible** for any lack of proper formalization between the Controller client, its EPSs, and registered employees. Any claims by data subjects must be initially directed to the Controller client, who is legally responsible for data processing decisions.

Cesla remains obligated to:

- Ensure retention of EPS and employee data for up to 20 years, exclusively when there is an active client Controller contract or a valid link to another active client;
- Maintain login records, audit trails, and traceability logs for at least 5 years, including after contract termination, for purposes of security, regulatory compliance, and the regular exercise of rights;
- Apply technical and organizational controls to ensure confidentiality, integrity, and availability of processed data;
- Support the Controller client in responding to data subject requests, as required by the LGPD.

12. Incident and Non-Compliance Reporting

All users of the Cesla platform — including contracting clients, Service Provider Companies (EPSs), and Cesla employees — must actively identify and report situations that may pose a risk to information security or LGPD compliance.

In the event of identification or suspicion of:

- Leakage or unauthorized access to personal data;
- Abnormal system behavior or relevant technical failures;
- Unauthorized data sharing;
- Misuse of credentials or access permissions;
- Contractual or legal non-compliance related to data processing;
- Security failures in authentication, permissions, or information integrity;
- Non-compliance with LGPD or contractual clauses;

The incident must be reported **immediately** to Cesla through official support channels or directly to the Data Protection Officer (DPO) at **dpo@intuix.com**.

Responsibilities

- **Cesla (Processor):**
  - Provides technical support in detecting, containing, analyzing, and recording the incident;
  - Supplies evidence and technical reports to the Controller client, including audit logs and traceability records retained for at least 5 years, even after contract termination;
  - Supports execution of the Incident Response Plan (IRP), ensuring traceability and documentation.

- **Contracting client (Controller):**
  - Is responsible for assessing the incident's impact on data subjects;
  - Decides whether official notification to affected data subjects and to the ANPD (National Data Protection Authority) is required, as provided by the LGPD;
  - Leads external communications (data subjects, regulators, partners), with Cesla's technical support when applicable.

The use, sharing, or storage of improperly accessed data is strictly prohibited. Any violation may result in civil, criminal, and contractual liability, in accordance with applicable law and the commitments made with data subjects.

13. Intellectual Property

All intellectual property rights related to the Cesla platform — including its modules, functionalities, interface, data structures, operational flows, brand, visual identity, source code, databases, and other technical components — are the exclusive property of Cesla Tecnologia.

It is strictly prohibited for any user, client Controller, EPS, or third party to:

- Reproduce, copy, modify, decompile, reverse engineer, or create derivative works based on any Cesla module or functionality;
- Use the platform for purposes not contractually authorized or outside the scope of the granted license;
- Transfer, assign, or sublicense the use of the platform without formal authorization from Cesla Tecnologia.

The contracting of the Cesla platform license grants the Controller client a non-exclusive, non-transferable right of use limited to the contractual term, as defined in the commercial agreement.

Misuse may result in civil, criminal, and administrative liability, in addition to sanctions provided for in the contract and applicable law.

This item does not affect the Controller client's rights over the personal and operational data entered into the platform, which remain under its ownership and legal responsibility, in accordance with the LGPD.

14. Data Protection Officer (DPO)

Cesla Tecnologia has appointed a Data Protection Officer (DPO), responsible for serving as a communication channel between Cesla, client Controllers, data subjects, the Brazilian National Data Protection Authority (ANPD), and other stakeholders.

Responsibilities of Cesla's DPO

- Act as a support contact point for client Controllers, providing technical and administrative guidance on data privacy and security;
- Assist clients in fulfilling data subject requests when received by Cesla, ensuring they are properly redirected to the responsible Controller;
- Maintain records of incidents and communications related to data processing, ensuring traceability and compliance;
- Guide Cesla employees and sub-processors on personal data protection practices;
- Oversee Cesla's compliance with contractual instructions and LGPD, working in alignment with the Controllers.

Communication with data subjects

- The contracting client (Controller) is the primary responsible party for responding to data subject requests (e.g., access, correction, deletion, objection).
- If Cesla receives a request directly from a data subject, it will be logged and forwarded to the client Controller, with technical support provided to ensure the request is handled within legal timeframes.

Official contact channel for Cesla's DPO: dpo@intuix.com

15. Updates and Revisions

This Privacy Policy will be reviewed periodically, at least annually, or whenever the following occur:

- Significant changes in applicable legislation, especially those related to personal data protection;
- Updates to Cesla platform services, features, or modules that affect data processing;
- Relevant changes in internal processes regarding information security, privacy, or data governance.

Responsibilities in updating

- **Cesla Tecnologia (Processor)** is responsible for keeping this Policy aligned with security standards, best practices, and contractual requirements, formally notifying client Controllers of any relevant changes.
- The **client Controller** is responsible for evaluating and, when necessary, informing the data subjects under their responsibility about changes that may impact their rights.

All versions of this Policy include **history and version control**. The most current version will always be available in Cesla's official channels, within a secure repository.

16. Confidentiality

All information and personal data processed on the Cesla platform are considered confidential and protected against unauthorized access, use, or disclosure.

Responsibilities of Cesla (Processor)

- Implement strict technical and administrative measures to preserve the confidentiality of data processed on behalf of the client Controller;
- Require confidentiality and security clauses from its employees and sub-processors (e.g., Azure, EVEO, Cloudflare, Firebase);
- Ensure traceability through audit logs and continuous monitoring of operations.

Responsibilities of the Client (Controller)

- Ensure that data entered into the platform is processed in compliance with the LGPD and used only for the legitimate purposes contractually defined;
- Ensure that its own employees, EPSs, and partners maintain the confidentiality of the data under its responsibility;
- Notify Cesla whenever confidentiality breaches or risks related to platform usage are identified.

Restrictions

It is prohibited for any user, employee, or third party to:

- Share or use data improperly accessed;
- Disclose information processed on the platform without the Controller's authorization;
- Reuse information for personal, commercial, or unauthorized purposes.

Violation of confidentiality obligations may result in administrative, civil, or criminal sanctions, as provided by the LGPD, applicable law, and the agreements established between the parties.

17. Final Provisions

This Privacy Policy aims to ensure transparency, security, and compliance in the processing of personal data carried out on the Cesla platform.

- The contracting client (Controller) is primarily responsible for decisions regarding personal data processing, including the definition of purposes, legal bases, retention periods, and communication with data subjects.
- Cesla Tecnologia (Processor) acts solely under the Controller's documented instructions, applying appropriate technical and organizational measures to protect data, support the fulfillment of data subject rights, and ensure operational traceability.
- The retention periods applied by the platform follow contractual and legal criteria:
    - 60 days for data availability after contract termination, before permanent deletion;
    - Up to 20 years for EPS and employee data, when linked to active clients or in compliance with labor and legal obligations;
    - 5 years for login records, audit trails, and traceability logs, including after contract termination, exclusively for security, regulatory compliance, and the regular exercise of rights.
- International data transfers are carried out solely in Cesla's role as Processor, using certified sub-processors (Azure, EVEO, Cloudflare, Firebase), always in compliance with the Controller's instructions and LGPD requirements.

Cesla is committed to keeping this Policy updated in accordance with legislation, international information security standards (ISO/IEC 27001, 27035), and the agreements established with its clients.

18. Review and Approval

This Privacy Policy has been reviewed and approved in accordance with Cesla Tecnologia's internal governance processes.

The periodic review ensures that the document remains aligned with the LGPD, international information security standards (e.g., ISO/IEC 27001, 27035), and agreements executed with clients.

Approval of this document does not alter the nature of responsibilities:

- The contracting client remains the **Controller** of the personal data entered into the platform;
- Cesla Tecnologia acts as the **Processor**, handling data in accordance with the Controller's documented instructions.

Responsible Parties

Technical Review:

- Silvia Adriana Silvestrini — Chief Product Officer (CPO)
    - Principal technical responsible person.

Executive Approval:

- Cleber Candido Eduardo — Chief Executive Officer (CEO)
    - Institutional responsible person.

Campinas/SP, August 22, 2025.

Documento assinado digitalmente
gov.br
SILVIA ADRIANA SILVESTRINI EDUARDO
Data: 01/09/2025 14:24:06-0300
Verifique em https://validar.iti.gov.br

Silvia Adriana Silvestrini
CPO – Chief Product Officer
Technical Responsible

Documento assinado digitalmente
gov.br
CLEBER CANDIDO EDUARDO
Data: 01/09/2025 14:52:30-0300
Verifique em https://validar.iti.gov.br

Cleber Candido Eduardo
CEO – Chief Executive Officer
Institucional Responsible