# RELATÓRIO DE DIAGNÓSTICO DE CONFORMIDADE LEGAL

## 1. INTRODUÇÃO

### 1.1. Objetivo

O trabalho teve por objetivo avaliar a conformidade da empresa em relação ao tratamento de dados pessoais, inclusive nos meios digitais, por pessoa jurídica de direito privado, no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD).

### 1.2. Contextualização

Considerando o crescente volume de dados tratados nos meios digitais e a importância da proteção da privacidade dos titulares, este trabalho buscou verificar se os processos internos da organização estão alinhados com as exigências legais quanto à coleta, armazenamento, uso, compartilhamento e descarte de dados pessoais. A análise abrangeu aspectos como a existência de políticas de privacidade, mecanismos de segurança da informação, registro de operações de tratamento, consentimento dos titulares e a atuação do encarregado pelo tratamento de dados (DPO), com vistas à mitigação de riscos e à promoção da transparência e responsabilidade no uso de informações pessoais.

### 1.3. Referências Legais

- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018.
- Constituição da República Federativa do Brasil de 1988.

### 1.4. Delimitação do Escopo

O trabalho foi realizado na empresa Cidadania4u, a qual oferece serviço de assessoria para o reconhecimento de cidadania europeia.

O método de avaliação foi realizado a partir de vinte e uma questões referentes ao processo simplificado para implementação da LGPD previsto na Cartilha elaborada pelo grupo.

A análise também teve como subsídio as respostas obtidas a perguntas em reunião de apresentação da Cartilha realizada na empresa no dia 23 de outubro de 2025.

## 2. RESULTADO DA AVALIÇÃO

A empresa apresentou resposta positiva para 14 questões, o que demonstra um nível de conformidade avançada em relação ao tratamento de dados pessoais previsto na LGPD.

Respostas negativas foram obtidas nas questões 1, 2, 8, 16, 17, 18 e 19, indicando a necessidade de implantação de um Comitê de Privacidade ou estrutura de governança para proteção de dados.

**Tabela 1** – Resumo das questões e respostas.

| Nº | Questão | Resposta |
|---|---|---|
| 1 | A empresa possui um Comitê de Privacidade ou estrutura de governança para proteção de dados? | Não |
| 2 | Foi nomeado um Encarregado de Proteção de Dados (DPO)? Ele está formalmente designado? | Não |
| 3 | Os colaboradores foram treinados sobre a LGPD e boas práticas de proteção de dados? | Sim |
| 4 | A empresa realizou o mapeamento dos dados pessoais que coleta e trata? | Sim |
| 5 | Existe um inventário atualizado com os tipos de dados, finalidades e bases legais? | Sim |
| 6 | Os dados pessoais são classificados por sensibilidade e risco? | Sim |
| 7 | A empresa possui políticas de privacidade internas e externas? | Sim |
| 8 | Há procedimentos documentados para coleta, uso, compartilhamento e descarte de dados? | Não |
| 9 | Os contratos com terceiros incluem cláusulas de proteção de dados? | Sim |
| 10 | Quais medidas técnicas foram adotadas para proteger os dados (ex.: criptografia, controle de acesso)? | Sim |
| 11 | Existe um plano de resposta a incidentes de segurança? | Sim |
| 12 | Os sistemas são auditados e atualizados regularmente? | Sim |
| 13 | A empresa possui canais para que os titulares exerçam seus direitos (acesso, correção, exclusão, portabilidade)? | Sim |
| 14 | Os pedidos dos titulares são registrados e atendidos dentro dos prazos legais? | Sim |
| 15 | O consentimento é coletado de forma clara e transparente, quando necessário? | Sim |
| 16 | A empresa elaborou Relatórios de Impacto à Proteção de Dados para atividades de alto risco? | Não |
| 17 | Há uma matriz de riscos que avalia impactos à privacidade? | Não |

| | | |
|---|---|---|
| 18 | Os riscos identificados foram tratados com medidas de mitigação? | Não |
| 19 | A conformidade com a LGPD é revisada periodicamente? | Não |
| 20 | Há indicadores ou métricas para acompanhar o desempenho do programa de privacidade? | Sim |
| 21 | A empresa acompanha atualizações da legislação e orientações da ANPD? | Sim |

## 3. RECOMENDAÇÕES

Tendo em vista os resultados obtidos, recomenda-se à empresa os seguintes procedimentos:

a. Implementação do Comitê de Privacidade e a nomeação do Encarregado de Proteção de Dados (DPO);

b. Elaboração do Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).

### 3.1. Implementação do Comitê de Privacidade

O Comitê de Privacidade deve envolver, dentro do possível, representantes das áreas jurídica, tecnologia da informação, compliance, segurança da informação, recursos humanos e operações. O Comitê deverá nomear um coordenador ou presidente, que atuará em conjunto com o encarregado pelo tratamento de dados (DPO).

Além disso, o comitê deve ser multidisciplinar, com membros que tenham autonomia decisória e conhecimento sobre o tratamento de dados. A presença do DPO (Encarregado de Dados) é altamente recomendada, mesmo que ele não seja o coordenador. A estrutura pode ser ajustada conforme a realidade organizacional, desde que garanta efetividade na implementação e fiscalização das políticas de privacidade.

A criação do comitê é uma medida estratégica que demonstra o compromisso da organização com a conformidade legal, a ética no tratamento de dados e a construção de confiança com clientes e parceiros.

A nomeação do DPO é essencial para evitar sanções legais, fortalecer a confiança dos clientes e garantir a transparência no uso de dados pessoais. Mesmo em empresas onde sua nomeação não é obrigatória, contar com um DPO é altamente recomendável.

Nesse sentido, a escolha do DPO deve recair na pessoa que disponha dos seguintes requisitos: ter conhecimento técnico e jurídico sobre proteção de dados pessoais e

privacidade; capacidade de comunicação com diferentes públicos: titulares de dados, autoridades reguladoras e áreas internas da organização; imparcialidade e autonomia para atuar com independência na fiscalização e orientação; visão estratégica para integrar a proteção de dados à cultura organizacional; habilidade de gestão de riscos e conformidade regulatória.

### 3.2. Elaboração do Relatórios de Impacto à Proteção de Dados Pessoais (RIPD)

O RIPD é um documento exigido pela LGPD (art. 38) que descreve as operações de tratamento de dados pessoais que podem representar alto risco aos direitos e liberdades dos titulares. Ele deve conter medidas de mitigação, salvaguardas e mecanismos de proteção.

O Controlador, que no caso pode ser um representante do Comitê de Privacidade, deve ser o agente de tratamento responsável pela elaboração do RIPD.

Conforme o art. 38 da LGPD, o RIPD deverá conter, pelo menos:

i. a descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma;

ii. a metodologia usada para o tratamento e para a garantia da segurança das informações; e

iii. a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

É importante que o relatório seja suficientemente detalhado, para que o próprio Controlador tenha compreensão ampla de como ocorre o tratamento dos dados pessoais e os possíveis riscos associados a ele.

Assim, recomenda-se ao Controlador descrever os tipos de dados pessoais tratados, as operações de tratamento (art. 5º, X, da LGPD), suas finalidades (incluindo interesses legítimos) e hipóteses legais, e avaliar a necessidade e a proporcionalidade das operações de tratamento, os riscos para os direitos e liberdades dos titulares de dados e as medidas a serem adotadas para minimizar esses riscos.

Por fim, recomenda-se elaborar o RIPD antes de o controlador iniciar o tratamento dos dados pessoais para a finalidade desejada, justamente para que ele possa avaliar, de antemão, os possíveis riscos associados a esse tratamento.

## 4. CONCLUSÃO

Conforme foi consignado nas páginas iniciais deste relatório, o trabalho chegou à conclusão, com base em exame processual e nas informações colhidas do gestor, de que a empresa possui um grau elevado de compliance em relação ao tratamento de dados pessoais previsto na LGPD.

Entretanto, foram identificadas possibilidade de melhorias na gestão de dados, as quais possibilitaram um maior compromisso da organização com a conformidade legal e a ética no tratamento de dados.

Assim, o trabalho concluiu pela recomendação apenas da implementação do Comitê de Privacidade, juntamente com a nomeação do Encarregado de Proteção de Dados (DPO), assim como a elaboração do Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).

**DECLARAÇÃO DE CONCORDÂNCIA E COMPROMISSO COM A GOVERNANÇA DE DADOS PESSOAIS**

A **Cidadania4u**, pessoa jurídica de direito privado, representada por Vitoria Borges da Silva, Assistente Backoffice, **declara que concorda com o conteúdo e as conclusões constantes do Relatório de Diagnóstico de Conformidade Legal**, elaborado pelos alunos da disciplina de Governança e Compliance do curso de Direito do Centro Universitário Uniprocessus, reconhecendo sua relevância para a mitigação de riscos regulatórios e para a promoção da conformidade normativa.

O referido relatório constitui instrumento essencial para a governança corporativa, pois identifica o grau de aderência às normas aplicáveis, aponta eventuais desconformidades e recomenda providências necessárias à observância dos princípios da legalidade, transparência e eficiência, previstos no ordenamento jurídico.

Adicionalmente, o órgão gestor **assume o compromisso de implementar medidas estruturantes de proteção de dados pessoais**, em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), consistentes em:

1. **Instituir um Comitê de Privacidade**, com atribuições voltadas à definição de diretrizes, acompanhamento da execução das políticas internas e promoção da cultura de proteção de dados na organização;
2. **Nomear um Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO)**, que atuará como canal de comunicação com os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), além de coordenar as ações de conformidade;
3. **Elaborar Relatórios de Impacto à Proteção de Dados Pessoais (RIPD)**, sempre que necessário, para avaliar riscos e impactos relacionados às operações de tratamento de dados, garantindo a adoção de medidas preventivas e corretivas.

Por fim, reafirma-se o compromisso institucional com a implementação das recomendações constantes do relatório e com a observância das normas legais aplicáveis, visando assegurar a conformidade regulatória e a proteção dos direitos dos titulares de dados pessoais.

Brasília, 18 de novembro de 2025.

gov.br Documento assinado digitalmente
VITORIA BORGES DA SILVA
Data: 18/11/2025 12:05:05-0300
Verifique em https://validar.iti.gov.br

Vitoria Borges da Silva, Assistente Backoffice