



POL-012 - Política de Proteção e Privacidade de Dados Pessoais

Sumário

| | |
|--|---|
| 1. Objetivo | 3 |
| 2. Definições referentes ao tratamento de dados pessoais | 3 |
| 3. Boas Práticas na Proteção de Dados Pessoais | 3 |
| 4. Direitos dos Titulares..... | 4 |
| 5. ERDOC como controladora - Coleta de dados pessoais | 4 |
| 6. ERDOC como operadora de dados pessoais | 5 |
| 7. Tratamento de dados pessoais | 5 |
| 7.1. Finalidade..... | 6 |
| 7.2. Bases legais | 6 |
| 7.3. Armazenamento e Segurança dos Dados | 7 |
| 7.4. Confidencialidade..... | 7 |
| 8. Compartilhamento | 7 |
| 8.1. Transferência internacional de DP | 8 |
| 8.2. Registros relativos ao tratamento de DP | 8 |
| 8.3. Avaliação de Impacto de Privacidade | 8 |
| 9. Treinamento e Conscientização | 8 |
| 10. Encarregado de Dados Pessoais - DPO | 8 |
| 11. Conformidade Legal..... | 9 |
| 12. Controle de Atualização | 9 |

1. Objetivo

Estabelecer os princípios e diretrizes para garantir a segurança e a confidencialidade dos dados pessoais coletados, processados e armazenados pela ERDOC, em conformidade com as leis e regulamentos aplicáveis.

Esta política se aplica a todos os dados pessoais coletados, processados e armazenados pela ERDOC em qualquer formato, incluindo eletrônico ou físico. Isso abrange informações coletadas por meio de sistemas, sites, aplicativos, formulários físicos, comunicações por telefone ou e-mail, entre outros meios.

2. Definições referentes ao tratamento de dados pessoais

- **Dado pessoal:** Informação relacionada a pessoa natural identificada ou identificável
- **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
- **Dado anonimizado:** Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
- **Titular:** 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
- **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador
- **Encarregado:** Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
- **Tratamento:** 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

3. Boas Práticas na Proteção de Dados Pessoais

Para garantir a conformidade com a legislação e a proteção dos dados pessoais tratados pela ERDOC, todos os colaboradores devem observar as seguintes diretrizes:

- Acessar dados pessoais somente quando necessário para o desempenho de suas funções.
- Utilizar credenciais individuais (login e senha) e nunca compartilhá-las
- Não divulgar, repassar ou comentar dados pessoais com pessoas não autorizadas, seja interna ou externamente
- Assinar e cumprir o Termo de Confidencialidade
- Utilizar apenas sistemas e ferramentas aprovados pela empresa para tratamento de dados pessoais
- Bloquear a tela ao se ausentar da estação de trabalho
- Armazenar documentos físicos com dados pessoais em locais seguros e trancados
- Evitar anotações que contenham dados pessoais em papéis ou dispositivos pessoais
- Usar criptografia ou canais seguros ao enviar dados pessoais por e-mail ou outro meio eletrônico
- Conferir destinatários antes de enviar mensagens com dados pessoais
- Coletar apenas os dados pessoais estritamente necessários para a finalidade pretendida
- Acionar sobre qualquer evento ou dúvida sobre tratamento de dados pessoais
- Não clicar em links suspeitos ou abrir anexos de origem desconhecida
- Comunicar imediatamente o Encarregado de Proteção de Dados (DPO) ou o time responsável qualquer incidente de segurança ou suspeita de vazamento de dados

- Descartar documentos físicos por meio de fragmentadoras ou serviços seguros de destruição
- Apagar arquivos digitais de forma definitiva, conforme orientação da área de TI
- Participar dos treinamentos periódicos sobre proteção de dados
- Manter-se atualizado sobre as políticas internas da empresa.

4. Direitos dos Titulares

O É considerado titular a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

A Lei Geral de Proteção de Dados (LGPD) define os seguintes direitos dos titulares:

- Confirmação da existência de tratamento
- Acesso aos dados; correção de dados incompletos, inexatos ou desatualizados
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei
- Portabilidade dos dados
- Eliminação dos dados
- Informação das entidades públicas e privadas que realizaram o compartilhamento de dados
- Informação sobre a possibilidade de não fornecer consentimento e as consequências dessa negativa
- Revogação do consentimento

A LGPD prevê a necessidade de um canal de comunicação seguro e acessível para que os titulares dos dados possam exercer seus direitos de privacidade e proteção de dados, garantindo que as solicitações sejam devidamente tratadas e respondidas em conformidade com as exigências da lei.

A ERDOC disponibiliza o e-mail protecaodedados@erdoc.com.br como canal de comunicação. O atendimento e tratamento das solicitações dos titulares dos dados pessoais serão realizados conforme “Procedimento de Atendimento à Requisição dos Titulares de dados pessoais”.

A ANPD pode entrar em contato com a ERDOC para apurar eventuais denúncias relacionadas a incidentes ou vazamento de dados pessoais.

5. ERDOC como controladora - Coleta de dados pessoais

A ERDOC, como controladora de dados pessoais, estabelece que os dados pessoais serão coletados de forma justa, legal e transparente, com o conhecimento e consentimento dos titulares, sempre que aplicável.

Serão coletados apenas os dados pessoais necessários para fins específicos e legítimos, e serão mantidas pelo tempo necessário para cumprir esses propósitos, conforme estabelecido nas leis e regulamentos aplicáveis.

No compartilhamento de Dados Pessoais com operadores, a relação deve ser regida por contratos, que estabeleçam garantias, responsabilidades e medidas necessárias de adequação à LGPD, bem como adoção das medidas apropriadas para o uso compartilhado de Dados Pessoais em consonância com os procedimentos de Privacidade e Proteção de Dados Pessoais.

6. ERDOC como operadora de dados pessoais

A ERDOC atua, em determinados processos, como operadora de dados pessoais, realizando o tratamento de dados pessoais de seus clientes, como instituições financeiras, bancos, administradoras de consórcios e demais controladores para viabilizar o registro e a gestão de contratos de financiamento de veículos na plataforma. O tratamento de dados pessoais é regido por contratos firmados com os controladores.

Para a execução de suas atividades como operadora, a ERDOC realiza integração com órgãos públicos, tais como o Departamento Estadual de Trânsito (DETRAN), visando à validação e conferência de dados relacionados a contratos de financiamento de veículos.

O acesso e o tratamento dos dados pessoais nesse contexto são realizados exclusivamente para atender às instruções dos controladores, com base legal prevista na legislação vigente, utilizando canais e protocolos de segurança definidos pelo órgão competente, e garantindo que tais informações não sejam utilizadas para finalidades distintas das contratadas.

A ERDOC não utiliza os dados pessoais tratados nessas atividades para finalidades próprias não autorizadas pelo controlador.

Quando atua como operadora, a ERDOC compromete-se a:

- Seguir estritamente as instruções do controlador no tratamento dos dados pessoais, abstendo-se de utilizá-los para finalidades próprias não autorizadas ou diferentes daquelas estabelecidas contratualmente.
- Garantir que a base legal para o tratamento esteja definida e comunicada de forma adequada.
- Adotar medidas técnicas e organizacionais adequadas para garantir a segurança, integridade, confidencialidade e disponibilidade das informações tratadas.
- Garantir a confidencialidade dos dados pessoais tratados, exigindo o mesmo compromisso de colaboradores, prestadores de serviço e parceiros envolvidos no processo.
- Manter registros das operações de tratamento realizadas em nome do controlador, conforme exigido pela legislação aplicável.
- Notificar o controlador imediatamente sobre incidentes de segurança que possam acarretar risco ou dano relevante aos titulares dos dados.
- Cooperar com o controlador no atendimento a solicitações dos titulares e no cumprimento de obrigações legais ou regulatórias.

7. Tratamento de dados pessoais

Deve-se considerar como tratamento de dados pessoais, toda operação realizada com dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Os dados pessoais devem ser coletados apenas na quantidade necessária para atender às finalidades específicas. A coleta excessiva deve ser evitada, e os dados coletados devem ser revisados e atualizados regularmente.

A ERDOC deve implementar processos para verificar a precisão dos dados e permitir que os titulares solicitem correções quando necessário, conforme “Procedimento de atendimento à requisição de titulares de dados pessoais”.

Quando necessário, devem ser estabelecidos objetivos de minimização dos dados pessoais, políticas e práticas para que seja realizada, de forma que não permita a identificação ou reidentificação dos titulares de DP.

Os dados pessoais devem ser anonimizados quando não forem mais necessários para o propósito original. Quando a anonimização não for possível, os dados devem ser excluídos de forma segura e eficaz ao término do tratamento.

Quaisquer dados armazenados temporariamente para processamento devem ser gerenciados para garantir que não sejam mantidos por mais tempo do que o necessário. Esses arquivos devem ser excluídos ou anonimizados assim que não forem mais necessários.

A ERDOC estabelece que os dados pessoais devem ser mantidos apenas pelo tempo necessário para cumprir as finalidades para as quais foram coletados, e em conformidade com as exigências legais.

Caso a ERDOC realize tratamento automatizado de dados pessoais, este deve ser comunicado aos titulares e jurisdições, permitindo aos titulares desaprovarem estas decisões tomadas, e/ou solicitar a intervenção humana.

Os dados pessoais que não são mais necessários devem ser descartados, incluindo a destruição física de documentos ou a eliminação segura de dados digitais, garantindo que não possam ser recuperados.

7.1. Finalidade

O tratamento de dados pessoais deve ser realizado com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Os dados devem ser tratados apenas para os propósitos e finalidades previamente identificados e documentados. Mudanças nas finalidades de tratamento devem ser justificadas e, se necessário, o consentimento dos titulares deve ser obtido novamente.

7.2. Bases legais

A Lei Geral de Proteção de Dados (LGPD) estabelece dez bases legais que justificam o tratamento de dados pessoais:

- **Consentimento** – Autorização dada pelo titular dos dados, concordando explicitamente com o tratamento de seus dados para uma finalidade específica.
O titular tem o direito de revogar o consentimento a qualquer momento, devendo ser informado sobre as consequências de sua negativa. Após a revogação, os dados devem ser eliminados, exceto em situações em que a continuidade do tratamento é fundamentada em outra base legal.
O controlador deve manter registros do consentimento, evidenciando que o titular concordou com o

tratamento, incluindo a data, a forma (digital ou física) e as finalidades específicas para as quais os dados serão usados.

- **Cumprimento de obrigação legal ou regulatória** – Cumprimento de obrigação legal ou regulatória à qual o controlador está sujeito.
- **Execução de contratos** – Execução de um contrato do qual o titular é parte, ou para a realização de procedimentos preliminares relacionados a um contrato.
- **Interesse legítimo** – Atendimento dos interesses legítimos do controlador ou de terceiros, desde que não sobreponham os direitos e liberdades fundamentais do titular.
- **Proteção da vida ou da incolumidade física** – Proteção da vida ou da incolumidade física do titular ou de terceiros.
- **Tutela da saúde** – Para fins de assistência médica, prevenção de doenças e promoção da saúde, realizado por profissionais da saúde ou por entidades de saúde.
- **Interesse público** – Exercício regular de direitos em processos administrativos e judiciais, ou para atender a uma função pública.
- **Estudo por órgão de pesquisa** – Realização de estudos por órgão de pesquisa, garantindo a anonimização dos dados sempre que possível.
- **Proteção ao crédito** – Proteção do crédito, conforme regulado por lei.
- **Exercício regular de direitos** – Exercício regular de direitos em processo judicial, administrativo ou em qualquer outra situação que envolva direitos e garantias

7.3. Armazenamento e Segurança dos Dados

Os dados pessoais devem ser armazenados de forma segura, com acesso restrito aos colaboradores autorizados e devem ser mantidos pelo tempo necessário para cumprir com as finalidades descritas nesta Política, ou pelo período exigido por lei. Após esse período, os dados serão deletados ou anonimizados.

As medidas de segurança incluem:

- Criptografia de dados sensíveis
- Controle de acesso aos sistemas que armazenam dados
- Políticas de backup regulares
- Treinamento contínuo de colaboradores sobre a segurança de dados

7.4. Confidencialidade

Todos os colaboradores, fornecedores e parceiros devem assinar um Termo de Confidencialidade, para garantir que as informações confidenciais não sejam compartilhadas e utilizadas de forma não autorizada.

8. Compartilhamento

O compartilhamento deve ser realizado de forma transparente e apenas quando necessário, sempre respeitando as bases legais estabelecidas pela LGPD. Ao compartilhar dados, devem ser adotadas medidas de segurança para proteger a privacidade dos titulares, e os terceiros envolvidos estarão obrigados a manter a confidencialidade e a proteger os dados conforme a legislação vigente. Além disso, os titulares devem ser previamente informados sobre qualquer compartilhamento, detalhando a finalidade e os destinatários dos dados.

Os dados pessoais que forem transmitidos devem ser protegidos através de medidas adequadas, como criptografia, e o acesso deve ser restrito a apenas aqueles que realmente precisam, garantindo que os dados sejam protegidos contra interceptações não autorizadas.

Devem ser mantidos registros detalhados de todas as transferências de dados pessoais, incluindo informações sobre o destinatário, a finalidade da transferência e a base legal utilizada, para garantir transparência e conformidade.

8.1. Transferência internacional de DP

Quando necessário, devem ser identificadas a finalidade e as bases legais que permitem a transferência de dados pessoais para fora do país, incluindo a adequação do país receptor quanto a privacidade e proteção de dados pessoais, cláusulas contratuais padrão, regras corporativas vinculativas ou consentimento explícito do titular.

A organização deve manter uma lista atualizada de países e organizações internacionais para os quais os dados podem ser transferidos, assegurando que estes ofereçam um nível de proteção de dados adequado, conforme a legislação aplicável.

8.2. Registros relativos ao tratamento de DP

Os registros de tratamento dos dados pessoais devem ser mantidos atualizados, incluindo informações sobre as atividades de tratamento, tipos de dados coletados, finalidades, bases legais, e uma descrição geral das medidas de segurança implementadas.

O mapeamento dos dados pessoais é realizado na ferramenta de mapeamento de dados pessoais, conforme “Procedimento de Mapeamento de dados pessoais”.

8.3. Avaliação de Impacto de Privacidade

Para cada tratamento realizado ou novo tratamento, devem ser identificados os riscos potenciais, controles existentes e as medidas necessárias para mitigá-los, assegurando que os direitos dos titulares sejam respeitados.

9. Treinamento e Conscientização

A ERDOC fornecerá treinamento e conscientização adequados aos seus funcionários e prestadores de serviços sobre a importância da proteção da privacidade e a conformidade com esta política. Os funcionários serão instruídos sobre as melhores práticas de manuseio dos dados pessoais e a importância de manter sua confidencialidade e segurança.

A ERDOC promoverá uma cultura de proteção de dados e privacidade, incentivando a adesão aos princípios desta política em todas as áreas da organização.

10. Encarregado de Dados Pessoais - DPO

Questões relacionadas à proteção e privacidade dos dados pessoais deverão ser tratadas diretamente com o Encarregado de dados pessoais (DPO). Os titulares podem entrar em contato com o ponto de contato para

fazer perguntas, exercer seus direitos de privacidade ou relatar preocupações relacionadas aos dados pessoais coletados e processados pela organização.

As responsabilidades do DPO envolvem:


- Garantir que a organização esteja em conformidade com as leis de proteção de dados vigentes e relevantes e com outras regulamentações de privacidade
- Oferecer orientação sobre como a organização deve interpretar e aplicar as leis de proteção de dados, bem como fornecer aconselhamento sobre as obrigações da organização em relação à privacidade
- Conscientizar os funcionários e a equipe sobre a importância da proteção de dados e fornecer treinamento para garantir o cumprimento das regulamentações
- Gerenciar e supervisionar a resposta a incidentes de segurança de dados, incluindo a notificação às autoridades reguladoras e às partes afetadas, quando necessário
- Auxiliar na realização de avaliações de impacto à proteção de dados sempre que operações de tratamento de dados possam apresentar riscos elevados para os direitos e liberdades dos titulares dos dados
- Facilitar a comunicação entre a organização e os titulares dos dados, permitindo que estes últimos exerçam seus direitos de proteção de dados
- Atuar como ponto de contato entre a organização e as autoridades de proteção de dados, facilitando a comunicação e a colaboração quando necessário
- Garantir que as regras e condições relacionadas a Proteção de Dados Pessoais e Política de Privacidade estabelecidas em contratos com colaboradores, clientes, fornecedores estejam em conformidade com as regulamentações de proteção de dados
- Realizar auditorias internas para garantir que os processos e procedimentos estejam alinhados com as regulamentações de proteção de dados
- Manter uma avaliação contínua dos riscos relacionados à proteção de dados e implementar medidas para mitigar esses riscos.

11.Conformidade Legal

A ERDOC está comprometida em cumprir todas as leis e regulamentos aplicáveis à proteção dos dados pessoais, incluindo, mas não se limitando a leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD).

A ERDOC cooperará com as autoridades reguladoras e responderá prontamente a qualquer violação de dados pessoais, conforme exigido por lei.

12.Controle de Atualização

| Data | Versão | Alteração | Responsável | Aprovação |
|------------|--------|-------------------------|-----------------|---|
| 05/08/2025 | 1.0 | Elaboração do documento | ASR Consultoria |  |
| | | | | |
| | | | | |