

## POLÍTICA DE GOVERNANÇA DE DADOS PESSOAIS

### 1. OBJETIVO

A Política de Governança de Dados (“Política”) do Eldorado tem como objetivos:

- Formalizar as diretrizes relacionadas ao tratamento dos dados pessoais e a importância da adoção das melhores práticas no Eldorado;
- Estabelecer as responsabilidades e os limites de atuação do Eldorado em relação à proteção aos dados pessoais, reforçando a cultura interna e priorizando as ações necessárias conforme o negócio;
- Formalizar o comprometimento do Eldorado em se adequar às leis aplicáveis, fortalecendo os negócios, as parcerias e as relações com os titulares dos dados pessoais.

### 2. APLICAÇÃO

Esta Política se aplica às atividades de todo e qualquer integrante do Eldorado, independentemente do seu nível hierárquico ou relação contratual, que realize atividades de tratamento de dados pessoais sob a responsabilidade do Eldorado.

As diretrizes deste documento se aplicam a todas as categorias de dados pessoais tratados pelo Eldorado, sejam seus titulares os colaboradores, prestadores de serviços, fornecedores, clientes, outros parceiros de negócios ou outras pessoas que venham a ter algum relacionamento com o Eldorado ou se envolvam em suas atividades.

### 3. DIVULGAÇÃO

Esta Política deve ser divulgada periodicamente a todos os colaboradores através dos meios institucionais de comunicação (ex: e-mails, intranet, murais eletrônicos etc).

Além disso, a Política deve estar disponível para consulta no Sistema de Gestão Integrado - SGQ ou poderá ser solicitada a qualquer momento ao Encarregado de Dados Pessoais através do e-mail [privacidade@eldorado.org.br](mailto:privacidade@eldorado.org.br).

### 4. DEFINIÇÕES

**Agente de tratamento:** É a pessoa natural ou pessoa jurídica, de direito público ou privado, responsável pela realização das atividades de tratamento de dados pessoais.

**Anonimização:** Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento para retirar a possibilidade de associação, direta ou indireta, do dado pessoal a um indivíduo.

**Banco de dados:** Conjunto estruturado de dados, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

**Ciclo de vida do dado pessoal:** Fluxo do tratamento do dado pessoal, que envolve as ações de Coleta, Armazenamento, Uso, Compartilhamento e Eliminação do dado pessoal.

**Compartilhamento de dados pessoais:** Comunicação, difusão, transferência nacional ou internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos, entidades ou pessoas, e para uma ou mais modalidades de tratamento.

**Confidencialidade:** Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não autorizados.

**Controlador:** Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

**Dado pessoal:** Informação relacionada à pessoa física identificada ou identificável. Para os propósitos desta Política, os dados pessoais são classificados como Informação Confidencial.

**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.

**Disponibilidade:** Garantia de que as informações e os recursos de tecnologia da informação e comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

**Encarregado pelo tratamento de dados pessoais:** Pessoa física ou jurídica indicada pelo Agente de Tratamento que atua como canal de comunicação com os titulares dos dados pessoais e com a Autoridade Nacional de Proteção de Dados (ANPD), conforme a LGPD e a Resolução CD/ANPD nº 18, de 16/07/2024.

**Incidente de segurança da informação:** Eventos de segurança da informação indesejados ou inesperados que têm uma probabilidade significativa de comprometer a integridade, a disponibilidade e a confidencialidade das informações de uma organização.

**Incidente de segurança da informação com dados pessoais:** É um evento adverso confirmado que comprometa a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais, conforme definição do artigo 3º, XII, da Resolução CD/ANPD nº 15/2024. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estão armazenados.

**Integridade:** Garantia de que as informações estejam fidedignas em relação à última alteração desejada durante o seu ciclo de vida.

**Operador:** Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

**Pseudonimização:** É o tratamento por meio do qual um dado pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

**Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC):** Hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

**Titular dos dados pessoais:** Pessoa física a quem se referem os dados pessoais que são objeto de tratamento.

**Tratamento de Dados Pessoais:** 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. Pode ser realizado por meios físicos ou digitais.

## 5. RESPONSABILIDADES

### 5.1 Alta liderança - Superintendente e Executivos

O Superintendente e os Executivos devem zelar para que o Eldorado adote as medidas técnicas e organizacionais adequadas à proteção de dados pessoais.

Assim, deverão aprovar, conforme Estatuto Social e procedimentos internos, os investimentos necessários em segurança da informação e proteção de dados pessoais, considerando a viabilidade, os custos, a técnica disponível e o tratamento de dados pessoais.

### 5.2 Encarregado pelo tratamento de dados pessoais

O Eldorado deverá manter em seus quadros um Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO), que terá ao menos as atividades e atribuições constantes dos artigos 15 e 16 da Resolução CD/ANPD nº 18, de 16/07/2024.

Atualmente a colaboradora Sarah Regina de Oliveira Campos exerce a função de Encarregada de Dados Pessoais com relação a todas as unidades do Eldorado.

Na sua ausência, sua substituta será: Anna Stela Basso Zito Lima.

### 5.3 Comitê de privacidade

No Eldorado o tema privacidade e proteção de dados é tratado dentro do Programa de Ética e Compliance. Assim, os assuntos e ações de conformidade relacionados a ele são debatidos e acompanhados pelo Comitê de Ética e Conformidade (IPE-0362-PRO).

### 5.4 Departamento de Tecnologia e Segurança da Informação (DTI) e Equipe de Sistemas Corporativos (ADS)

No que se refere à proteção de dados pessoais, caberá ao DTI e ADS:

- Promover a cultura de segurança da informação no Eldorado;
- Definir controles de segurança da informação para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais tratados pelo Eldorado;
- Assegurar continuamente que todos os sistemas e equipamentos corporativos usados para o tratamento de dados pessoais estejam dentro de um padrão aceitável de segurança;
- Analisar os aspectos técnicos de produto ou serviço de terceiros que o Eldorado esteja considerando contratar para processar ou armazenar dados pessoais para fins corporativos (exemplos: nuvem, hardware, equipamentos de rede);
- Atuar de forma coordenada com o Encarregado pelo Tratamento de Dados Pessoais para viabilizar a implementação de medidas técnicas e organizacionais de segurança da informação adequadas para o tratamento de dados pessoais;
- No âmbito de suas atividades e atribuições, coletar e manter registros das atividades de tratamento de dados pessoais, envolvendo, por exemplo, logs; controle de acessos físicos ou lógicos; utilização da rede e de softwares corporativos; identificação de usuários, dentre outros.;
- Mapear riscos organizacionais relacionados a segurança das informações do Eldorado, incluindo dados pessoais;

- Manter um plano de gerenciamento e registro de incidentes de segurança da informação e auxiliar na análise e definição da criticidade de eventual incidente de segurança que envolva dados pessoais.

### **5.5 Departamento Jurídico (DJR)**

São responsabilidades do DJR quanto à privacidade e proteção de dados pessoais:

- Validar, com o apoio do Encarregado pelo Tratamento de Dados Pessoais, as minutas de contrato envolvendo o Eldorado visando que contenham as disposições adequadas sobre proteção de dados pessoais;
- Apoiar o Encarregado pelo Tratamento de Dados Pessoais na análise e interpretação de outras leis ou normas, nacionais ou internacionais, correlatadas a proteção de dados;
- Auxiliar o Encarregado pelo Tratamento de Dados Pessoais na elaboração de comunicados, respostas ou outra documentação direcionada à Agência Nacional de Proteção de Dados ou a outra autoridade competente;
- Colaborar na orientação dos integrantes do Eldorado quanto a importância de cumprimento dos dispositivos legais sobre proteção de dados, bem como quanto às medidas que devem ser adotadas no caso de ocorrência de um incidente de violação de dados pessoais.

### **5.6 Departamento de Recursos Humanos (DRH)**

O tratamento de dados pessoais é inerente às atividades de gestão de recursos humanos. Assim, cabe ao DRH:

- Promover a cultura de proteção de dados pessoais no Eldorado;
- Assegurar, com o apoio do Encarregado pelo Tratamento de Dados Pessoais, controles e/ou salvaguardas para o tratamento de dados pessoais nos processos relacionados ao DRH (ex: seleção; contratação; desligamento; modificação de atividades, incluindo a promoção; fornecimento de benefícios, dentre outros processos);
- Assegurar que cláusulas de confidencialidade e proteção de dados constem dos contratos assinados pelos colaboradores;
- Assegurar que os colaboradores façam sua opção, autorizando ou não o uso de sua imagem pelo Eldorado, através de termo eletrônico específico para tal finalidade;

### **5.7 Gestores**

Para fins desta Política, são considerados como gestores os PLs/Coordenadores e os DTLs/Gerentes, os quais possuem as seguintes responsabilidades com relação à proteção de dados pessoais:

- Promover a cultura de proteção de dados pessoais em suas equipes;
- Cumprir e fazer cumprir, junto a sua equipe, as diretrizes desta Política e demais procedimentos internos sobre o tema;
- Assegurar gestão de acesso adequada, de modo que seus colaboradores acessem e usem dados pessoais apenas quando autorizados e na medida de suas atividades/responsabilidades;
- Atuar em parceria com o Encarregado pelo Tratamento de Dados Pessoais para identificar as vulnerabilidades e ameaças à proteção de dados pessoais nos processos e atividades da sua área;

- Com o apoio do Encarregado pelo Tratamento de Dados Pessoais e do Departamento Jurídico, obter garantias (acordo de confidencialidade, cláusulas contratuais, dentre outras) de seus parceiros de negócios sobre o cumprimento da legislação pertinente a tratamento e proteção de dados pessoais;
- Atualizar o inventário de dados de sua área sempre que requisitado pelo Encarregado pelo Tratamento de Dados Pessoais.

### **5.8 Colaboradores em geral**

Cabe a cada colaborador do Eldorado:

- Cumprir e manter-se atualizado com relação a esta Política e demais procedimentos internos sobre o tema;
- Tratar os dados pessoais sob responsabilidade do Eldorado somente para fins autorizados, de forma ética e lícita, respeitando os direitos do titular dos dados pessoais e de acordo com as orientações desta Política e da legislação aplicável;
- Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente, por meio físico ou digital, em qualquer local ou mídia, inclusive na Internet;
- Ao identificar um incidente de segurança envolvendo dados pessoais, comunicar o Encarregado pelo Tratamento de Dados Pessoais imediatamente através do e-mail [privacidade@eldorado.org.br](mailto:privacidade@eldorado.org.br).

## **6. PRINCÍPIOS**

Para uma adequada atividade de tratamento de dados pessoais (ordinários ou sensíveis), é necessário respeitar os princípios de tratamento previstos no artigo 6º da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), os quais estão detalhados a seguir.

### **6.1 Transparência**

Este princípio determina que qualquer informação ou comunicação relacionada ao tratamento de dados pessoais seja concisa, compreensível e facilmente acessível em termos simples e claros. Isso significa que ao tratar dados pessoais, o Eldorado deve fornecer aos titulares dos dados informações claras sobre como seus dados serão tratados, qual é a finalidade do tratamento e quem será o responsável por ele. Em resumo, a transparência visa garantir que os titulares dos dados estejam bem informados sobre o uso de suas informações pessoais.

### **6.2 Proporcionalidade e necessidade**

As áreas que realizam o tratamento de dados pessoais devem buscar tratar o menor volume possível de dados, devendo esse volume ser proporcional às suas atividades e aos objetivos do negócio.

Assim, este princípio determina que o tratamento de dados pessoais realizado pelo Eldorado seja limitado ao mínimo necessário para atingir suas finalidades, considerando dados pertinentes e proporcionais, evitando-se o tratamento excessivo de informações pessoais. Esse princípio também é conhecido como princípio da razoabilidade e assegura que a utilização dos dados seja justa e adequada.

### **6.3 Finalidade e adequação**

Os dados pessoais devem ser tratados apenas para as finalidades determinadas, explícitas, legítimas e informadas antes do tratamento, não podendo ser tratados posteriormente para finalidades incompatíveis.

Os dados pessoais devem ser tratados de modo adequado e pertinente às suas finalidades de uso.

#### **6.4 Livre acesso e qualidade dos dados**

O Eldorado deve permitir aos titulares a consulta gratuita sobre quais dados são tratados e como eles são tratados.

Além disso, deve-se assegurar a exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

#### **6.5 Segurança e prevenção**

O tratamento realizado pelo Eldorado deve garantir a proteção e segurança dos dados pessoais, incluindo a proteção contra o tratamento não autorizado ou ilícito, perda, destruição ou dano acidental.

Desse modo, deve-se adotar medidas técnicas e organizacionais para salvaguardar a integridade, confidencialidade, disponibilidade e autenticidade dos dados pessoais, evitando-se qualquer dano ao titular.

#### **6.6 Não discriminação**

Em nenhuma hipótese o tratamento de dados deve ser executado para fins discriminatórios, ilícitos ou abusivos.

#### **6.7 Responsabilização e prestação de contas**

O Eldorado deve guardar provas e evidências de todas as medidas de proteção e segurança da informação adotadas, no sentido de demonstrar sua boa-fé e sua diligência.

### **7. DIRETRIZES**

De maneira geral, ao tratar dados pessoais, as seguintes diretrizes gerais devem ser observadas pelos integrantes do Eldorado:

- (i) Coletar apenas os dados mínimos necessários para a execução da finalidade pretendida.
- (ii) Informar ao titular, de maneira clara, a finalidade da coleta/tratamento dos dados pessoais.
- (iii) Utilizar os dados coletados apenas para a finalidade informada. Caso pretenda tratar os dados para outro fim, informe novamente o titular.
- (iv) Excluir os dados tão logo não sejam mais necessários, de modo a evitar o uso e armazenamento ilegal de dados pessoais.

A seguir, os elementos envolvidos nessas diretrizes são tratados de forma detalhada.

#### **7.1 Agentes de tratamento**

A LGPD estabelece que o tratamento de dados pessoais é toda operação realizada com dados pessoais, por meios físicos ou digitais, 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.

Ainda segundo a LGPD, os agentes que tratam dados pessoais são: o Controlador e o Operador de dados.

O Controlador é a pessoa física ou jurídica, de direito público ou privado, que coleta os dados e a quem competem as decisões referentes ao tratamento de dados pessoais. É o controlador que demanda o tratamento, podendo ele mesmo realizá-lo ou contratar um Operador (cuja definição veremos logo a seguir).

O Controlador deve realizar o tratamento de dados de acordo com a legislação e, se for o caso, orientar corretamente o Operador para que este realize um tratamento lícito.

Com relação à sua responsabilidade, o Controlador responde pelos danos patrimoniais, morais, individuais ou coletivos, tal como violações à legislação (dever de reparação). Ainda, responde solidariamente pelos danos causados pelo operador, se diretamente envolvido no tratamento que resultar em danos.

O Operador é a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, devendo, portanto, seguir as diretrizes estabelecidas pelo Controlador, além dos dispositivos legais.

Ele responde pelos danos patrimoniais, morais, individuais ou coletivos, tal como violações à legislação (dever de reparação) – assim como o Controlador. Responde, ainda, solidariamente caso descumpra a legislação (equiparando-se ao Controlador, caso não tenha seguido as instruções deste).

O Eldorado pode figurar ora como Controlador ora como Operador de dados pessoais, a depender da forma e do motivo do tratamento.

## **7.2 Minimização**

Os dados pessoais tratados pelo Eldorado devem ser limitados ao necessário para execução das finalidades de tratamento. Não se deve coletar dados pessoais excessivos, ou seja, que não possuam uma finalidade definida.

Deve-se sempre buscar formas alternativas (subsidiárias) de se atingir as mesmas finalidades por meios menos invasivos à privacidade do titular dos dados pessoais.

## **7.3 Hipóteses de tratamento**

O tratamento dos dados pessoais deve ser realizado de modo lícito, justo e transparente com relação ao titular dos dados pessoais.

O tratamento de dados pessoais somente é permitido e, portanto, está legitimado nas seguintes hipóteses indicadas no artigo 7º da LGPD:

- Em caso do cumprimento de uma obrigação legal ou regulatória do Eldorado;
- Quando o titular dos dados pessoais é parte em contrato ou os seus dados pessoais são necessários para execução de procedimentos preliminares para se firmar o contrato;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, prezando sempre pelo pedido de sigilo quando envolver dado pessoal;
- Para a proteção da vida ou da segurança física da pessoa a quem os dados pessoais se referem;
- Para proteção da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;
- Por interesse legítimo do Eldorado ou de terceiros, sendo obrigatória a confecção de relatório de impacto à proteção de dados pessoais. O tratamento com base no legítimo interesse deverá ser previamente analisado pelo Encarregado de Dados Pessoais.
- Não havendo enquadramento em nenhuma das hipóteses acima, mediante o consentimento do titular dos dados pessoais. É vedado o tratamento de dados pessoais mediante vício de consentimento. Sobre a obtenção e legitimação do consentimento do titular de dados, consulte o documento específico - IPE-0525-PRO.

#### **7.4 Consentimento**

Consentimento é o aceite; a concordância; a manifestação livre, informada e inequívoca pela qual o titular dos dados pessoais concorda com o tratamento de seus dados pessoais para uma finalidade determinada e claramente informada. Frisa-se que a obtenção e a legitimação do consentimento do titular são tratadas de forma detalhada no Procedimento IPE-0525-PRO.

Quando o tratamento dos dados pessoais se basear no consentimento do titular, este deve ser dado mediante manifestação de vontade livre de que o titular concorda com o tratamento de dados pessoais da forma declarada.

O consentimento pode ser dado de modo escrito, digital ou oral, sendo fundamental que se guarde sua evidência.

O consentimento para tratamento de dados pessoais sensíveis, deve ser coletado de forma específica e destacada, para finalidades específicas.

O silêncio, opções pré-validadas, generalistas ou a omissão NÃO são consideradas manifestações de consentimento.

O Eldorado deve realizar a gestão do consentimento nos casos em que o tratamento ocorrer com base nessa hipótese legal.

Se o consentimento do titular dos dados pessoais for dado no contexto de uma declaração escrita que diga também respeito a outras finalidades de tratamento, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente das demais finalidades de modo inteligível, destacado, de fácil acesso e em linguagem clara e simples.

O titular dos dados pessoais deve ser informado previamente sobre o direito de revogar o seu consentimento a qualquer momento e sobre eventuais consequências de tal anulação.

A revogação do consentimento deve ser oferecida de maneira simples, clara e facilitada, de preferência pela mesma via de coleta do consentimento, sendo certo que a retirada da autorização não compromete a licitude do tratamento já efetuado com base no consentimento previamente dado.

O tratamento de dados pessoais de crianças e adolescentes (menores de 18 anos incompletos), bem como eventual compartilhamento de tais dados, só devem ocorrer mediante o consentimento dado por pelo menos um dos pais ou pelo responsável legal.

#### **7.5 Uso**

O uso dos dados pessoais deve ser realizado dentro dos limites das finalidades informadas na coleta.

Caso haja a necessidade de realizar o tratamento do dado pessoal para outra finalidade (diversa da informada no momento da coleta), o titular dos dados pessoais deve ser informado de forma específica sobre o teor do novo tratamento e a possibilidade de revogar o consentimento caso não esteja de acordo com ele.



## 7.6 Armazenamento

O armazenamento dos dados pessoais pode ser feito de modo físico (guarda de crachás, cartões, fichas, papéis com anotações à mão, formulários, notas fiscais, contratos e outros documentos em papel, por exemplo) ou digital (em mídias como CD, DVD, Blu-Ray, HD externo, pendrive, cartão de memória SD, plataformas ou em serviços digitais contratado para esta finalidade).

No caso de armazenamento fora do Brasil, a área/departamento responsável pelo processo de negócio que envolva o tratamento dos dados pessoais deve estar atenta para o país em que a base de dados está localizada e deve acionar o Encarregado de Dados e/ou o Departamento Jurídico do Eldorado para verificar se há amparo legal e contratual para que os dados pessoais estejam armazenados nesse local.

Os meios físicos e digitais de armazenamento dos dados pessoais devem assegurar a qualidade dos dados, devendo ser mantidos exatos e atualizados, de acordo com a necessidade para o cumprimento da finalidade de tratamento.

Quando o titular dos dados pessoais solicitar a correção ou atualização de seus dados pessoais, o Encarregado de Dados Pessoais, após análise da requisição, deve acionar a área/departamento responsável para assegurar que os meios físicos e digitais onde esses dados pessoais foram replicados e armazenados sejam também atualizados.

Com relação ao prazo de retenção, os dados pessoais e seus respectivos registros devem ser armazenados apenas durante o período estritamente necessário de acordo com sua finalidade e a legislação pertinente.

Caso haja alguma dúvida com relação ao período indicado para armazenamento (retenção) dos dados pessoais, entre em contato com o Encarregado de Dados e/ou com o Departamento Jurídico.

## 7.7 Compartilhamento

O compartilhamento de dados pessoais tratados pelo Eldorado pode ocorrer nas seguintes hipóteses:

- (i) De forma automática, com nossas filiais;
- (ii) Para resguardar os direitos e/ou segurança do Eldorado, dos seus colaboradores e parceiros de negócios;
- (iii) Quando necessário para cumprimento de obrigação legal, regulatória, normativa ou ordem de autoridade competente;
- (iv) Quando necessário para a execução de atividades e/ou fornecimento de benefícios decorrentes do vínculo de trabalho ou emprego;
- (v) Quando necessário para a prestação de serviços ligados à segurança da informação.

Para compartilhamento de dados pessoais com outras empresas/organizações/órgãos fora das hipóteses mencionadas acima, deve-se observar as seguintes regras:

- As atividades desenvolvidas por tais empresas/organizações/órgãos devem estar ligadas à finalidade para qual os dados foram obtidos.
- Haja autorização do parceiro de negócios sempre que tal obrigação estiver prevista em contrato;
- Haja informação ao titular dos dados quando exigido pela LGPD.

Além disso, o compartilhamento de dados só deve ocorrer se houver garantias formais (acordo de confidencialidade, cláusulas contratuais, dentre outras) de cumprimento, pelo receptor, das diretrizes e leis de segurança e proteção de dados.

O compartilhamento de dados pessoais deve ocorrer somente por meios que tenham controles de segurança devidamente aplicados. Caso haja alguma dúvida com relação a este aspecto, deve-se solicitar uma avaliação do Departamento de Tecnologia e Segurança da Informação (DTI).

Dados pessoais anonimizados podem ser transferidos para terceiros.

### **7.8 Transferência internacional de dados pessoais**

A transferência internacional de dados pessoais é autorizada nas hipóteses do artigo 33 da LGPD.

Caso os dados pessoais tenham a previsão de serem transferidos para outro país e a transferência não se enquadre em nenhuma das hipóteses do artigo mencionado acima, entre em contato com o Encarregado de Dados antes de efetuar a transferência em questão para análise das medidas a serem adotadas para garantir a conformidade da ação.

### **7.9 Eliminação dos dados pessoais**

Os dados pessoais devem ser armazenados por período limitado, levando em consideração a finalidade específica do tratamento.

Após cumprida a finalidade do tratamento e findo o prazo de armazenamento, os dados devem ser eliminados de modo seguro, sejam eles registrados em meios físicos ou digitais.

Em determinadas situações, a eliminação dos dados pessoais também poderá ser realizada a pedido do titular do dado ou da Autoridade Nacional de Proteção de Dados.

Caso haja alguma dúvida sobre a forma de descarte, se ela é segura e adequada, consulte o Departamento de Tecnologia e Segurança da Informação.

A manutenção dos dados pessoais após atingida sua finalidade é possível no caso de cumprimento de obrigação legal/regulatória/normativa por parte do Eldorado ou se os dados forem anonimizados.

### **7.10 Dados pessoais sensíveis**

Dado pessoal sensível é o dado 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 física.

O tratamento de tais dados poderá ocorrer sem o consentimento do titular apenas nas seguintes hipóteses previstas no artigo 11 da LGPD:

- (i) Cumprimento de obrigação legal ou regulatória pelo Eldorado;
- (ii) Tratamento compartilhado de dados pessoais pela administração pública, necessários para execução de políticas públicas previstas em leis ou regulamentos;
- (iii) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- (iv) Proteção da vida ou da incolumidade física do titular ou terceiro;
- (v) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- (vi) Garantia de prevenção à fraude e segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (hipótese de legitimação exclusiva da lei de proteção de dados pessoais brasileira, aplicável, portanto, somente no território nacional).

Para qualquer outra situação de tratamento de dado pessoal sensível há necessidade de coleta do consentimento do titular, de forma específica e destacada, para finalidades determinadas. Frisa-se que a obtenção e a legitimação do consentimento do titular são tratadas de forma detalhada no Procedimento IPE-0525-PRO.

O tratamento de dados pessoais sensíveis deve ser precedido de relatório de impacto à proteção de dados pessoais, portanto, solicite previamente o apoio do Encarregado de Dados.

### **7.11 Dados de saúde**

Dados de saúde são dados pessoais sensíveis que permitem inferir informações referentes à saúde do titular.

Nos termos do artigo 11, §4º, da LGPD, tais dados podem ser compartilhados entre Controladores levando em consideração o benefício dos interesses dos titulares e se for realizado, exclusivamente, para:

- (i) Prestação de serviços de saúde e de seguros;
- (ii) Assistência farmacêutica;
- (iii) Assistência à saúde;
- (iv) Serviços auxiliares de diagnose;
- (v) Serviços de terapia.

Para outras hipóteses de compartilhamento de dados pessoais sensíveis, ainda que entre controladores, é necessário obter o consentimento do titular.

### **7.12 Decisões automatizadas**

Decisão automatizada é o processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou score, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, inteligência artificial, aprendizado de máquina, ou outra técnica computacional.

As áreas/departamentos do Eldorado devem listar os processos sob sua responsabilidade que envolvem decisões automatizadas baseadas no tratamento de dados pessoais, sempre se atentando para as seguintes premissas:

- Toda decisão automatizada que envolve o tratamento de dados pessoais deve disponibilizar informações claras e adequadas aos titulares sobre os seguintes aspectos, respeitados os segredos comercial e industrial: (i) os critérios utilizados para a tomada de decisão automatizada e (ii) os procedimentos utilizados para a tomada de decisão automatizada.
- O titular tem o direito de solicitar a revisão da tomada de decisão baseada em tratamento automatizado de dados pessoais, não sendo exigido que esta revisão seja realizada por pessoa natural.

### **7.13 Contratos**

Ao celebrar um contrato (ou outro documento negocial), deve-se analisar se para a realização do escopo haverá tratamento de dados pessoais pelas partes envolvidas. Se houver, o documento deverá conter disposições adequadas acerca do cumprimento da legislação de proteção de dados pessoais.

Se o Eldorado for firmar uma parceria ou fazer negócio com uma organização que vá figurar como Operadora de dados, ou seja, receberá dados pessoais compartilhados pelo Eldorado para executar seu serviço, as diretrizes/cláusulas sobre proteção de dados deverão ser ainda

mais claras já que Operador deve agir de acordo com as diretrizes estabelecidas pelo Controlador. Assim, é recomendável que os seguintes aspectos sobre o tratamento constem do contrato celebrado entre o Eldorado e a organização que processará os dados pessoais em seu nome:

- Finalidade e duração do tratamento pelo Operador;
- Categorias de dados pessoais envolvidos;
- Categorias de titulares envolvidos;
- Forma de armazenamento dos dados pessoais;
- Necessidade de autorização do Eldorado quanto à subcontratação de Operadores;
- Adoção de medidas de anonimização, pseudonimização (quando aplicável) e criptografia dos dados pessoais conforme a necessidade do tratamento em questão.

Caso haja alguma dúvida com relação às disposições que devem constar dos contratos ou outros documentos negociais celebrados pelo Eldorado, entre em contato com o Encarregado de Dados e/ou com o Departamento Jurídico.

#### **7.14 Segurança da informação**

Durante todo ciclo de vida do dado pessoal devem ser observadas as diretrizes de segurança da informação do Eldorado, as quais estão dispostas nas políticas e procedimentos do Departamento de Tecnologia e Segurança da Informação (DTI).

#### **7.15 Registros e evidências**

Cada área/departamento do Eldorado que trate dados pessoais é responsável por manter registros e/ou evidências do cumprimento das diretrizes desta Política para fins de evidências/registros organizacionais.

#### **7.16 Gestão de riscos**

O Sistema de Gestão de Riscos do Eldorado está documentado no documento organizacional IPE-0575-PRO que estabelece as diretrizes e procedimentos que devem ser seguidos pelo Eldorado para o desenvolvimento e manutenção de um processo estruturado e contínuo de identificação e gerenciamento de riscos.

Assim, riscos relacionais à proteção e tratamento de dados pessoais devem ser mapeados, classificados e tratados de acordo com as diretrizes do IPE-0575-PRO.

#### **7.17 Dúvidas**

Em caso de dúvidas quanto às diretrizes estabelecidas nesta Política, entre em contato com a Sarah Regina de Oliveira Campos, Encarregada de Dados do Eldorado, pelo e-mail [privacidade@eldorado.org.br](mailto:privacidade@eldorado.org.br).

### **8. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS**

Quando o Eldorado atuar como Controlador e (i) tratar dados pessoais tendo como base legal o legítimo interesse ou (ii) tratar dados pessoais sensíveis, deverá elaborar um relatório de impacto à proteção de dados pessoais.

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é o documento que contém a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares dos dados pessoais, bem como

medidas, salvaguardas e mecanismos de mitigação desses riscos. Tal relatório visa a descrição dos processos de tratamento de dados pessoais e as medidas e mecanismos empregados pelo Eldorado para mitigar riscos.

O RIPD deve ser elaborado pela área/departamento responsável pelo tratamento de dados pessoais em conjunto com o Encarregado de Dados, que poderá envolver outras áreas que sejam necessárias para entendimento, avaliação e elaboração do relatório.

## 9. ATENDIMENTO AOS TITULARES

Os titulares dos dados pessoais tratados pelo Eldorado possuem os direitos elencados abaixo, sendo que, ao figurar como Controlador, cabe ao Eldorado disponibilizar mecanismos para que eles sejam atendidos de maneira adequada:

- (i) **Confirmação do tratamento:** O titular poderá solicitar a confirmação do tratamento de seus dados pessoais pelo LET, bem como solicitar a exibição dos dados tratados. O prazo para atendimento desta solicitação é de quinze dias, conforme artigo 19, II, da LGPD.
- (ii) **Retificação e atualização de dados:** Se o titular identificar que os seus dados pessoais necessitam de correções ou se encontrarem incompletos, inexatos ou desatualizados, ele poderá solicitar a retificação/atualização ou, quando este recurso estiver disponível, poderá fazê-lo diretamente em um portal/sistema/plataforma disponibilizado pelo Eldorado.
- (iii) **Revogação do consentimento:** Caso o tratamento de dados pessoais pelo Eldorado tenha se dado com base no consentimento do titular, ele poderá, a qualquer momento, solicitar a revogação de tal autorização. Caso a revogação impacte o funcionamento (ainda que parcial) de algum serviço ou produto fornecido pelo Eldorado ao titular, ele deverá ser avisado sobre tal fato. Neste caso, também é importante que o titular fique ciente que a revogação do consentimento não significa que seus dados pessoais serão imediatamente eliminados pelo Eldorado, tendo em vista a possibilidade de conservação autorizada dos dados para as finalidades dispostas nas leis aplicáveis.
- (iv) **Anonimização, bloqueio ou eliminação de dados:** O titular poderá solicitar a anonimização, o bloqueio ou a eliminação dos seus dados pessoais tratados de maneira desnecessária, excessiva ou em desconformidade com esta Política.
- (v) **Portabilidade:** O titular pode solicitar a portabilidade de seus dados pessoais a outro fornecedor de serviços. Atualmente tal recurso está regulamentado apenas para planos de saúde e telefonia.
- (vi) **Informação sobre a possibilidade de não fornecer o seu consentimento:** Quando o tratamento de dados pessoais se der com base no consentimento, o titular deve ser claramente informado sobre eventuais consequências negativas caso decida não autorizar o tratamento.
- (vii) **Informação sobre compartilhamento:** O titular pode solicitar maiores informações sobre o compartilhamento de dados pessoais informado nesta Política.

O titular que desejar fazer alguma solicitação, precisar de esclarecimento ou de auxílio para exercer seus direitos, poderá entrar em contato direto com a Encarregada de Proteção de Dados Pessoais, Sarah Regina de Oliveira Campos, através do e-mail: [privacidade@eldorado.org.br](mailto:privacidade@eldorado.org.br). De acordo com os artigos 2º, V, e 15, I, da Resolução CD/ANPD nº 18, de 16/07/2024, o Encarregado é pessoa indicada para atuar como canal de comunicação entre o Agente de Tratamento e os titulares dos dados.

Caso um titular de dados entre em contato por outro meio/canal para exercer seus direitos, o receptor da solicitação deve notificar o Encarregado de Dados Pessoais, sem demora injustificada, que, então, analisará e responderá o pedido, sempre assegurando que a identidade do titular seja comprovada.

O Eldorado deverá envidar todos os esforços para atender os pedidos dos titulares no menor prazo possível, se atentando, também, para o cumprimento dos prazos estabelecidos pelas leis e regulamentos aplicáveis.

Ao atuar como Operador de dados, o Eldorado deverá contribuir com o Controlador, sempre que solicitado e no âmbito de sua atuação, para que os direitos dos titulares sejam atendidos.

## **10. COMUNICAÇÃO COM ÓRGÃOS DE CONTROLE**

### **10.1 Autoridade Nacional de Proteção de Dados (ANPD)**

A ANPD é um órgão da administração pública federal com autonomia técnica e decisória, responsável por fiscalizar e garantir o cumprimento da LGPD, bem como por aplicar sanções administrativas em caso de descumprimento.

Em caso de recebimento de notificação/requisição ou qualquer outra comunicação da ANPD, deve-se notificar o Encarregado de Dados Pessoais, que, com o apoio do Departamento Jurídico e sem demora injustificada, analisará a notificação/requisição/comunicação e elaborará a resposta à ANPD. Para a elaboração da resposta pode ser necessária a coleta de subsídios/informações junto a outras áreas/departamento do Eldorado ou, até mesmo, junto a parceiros de negócios.

### **10.2 Outros órgãos**

Se houver o recebimento de notificação/requisição/comunicação sobre privacidade e proteção de dados emitida por outra autoridade, seja ela judicial ou administrativa, deve-se notificar o Encarregado de Dados Pessoais e o Departamento Jurídico, sem demora injustificada, que, então, analisarão a notificação/requisição/comunicação e elaborarão a resposta adequada. Para a elaboração da resposta pode ser necessária a coleta de subsídios/informações junto a outras áreas/departamento do Eldorado ou, até mesmo, junto a parceiros de negócios.

## **11. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS**

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

A LGPD determina que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Os procedimentos internos relativos a incidentes de segurança com dados pessoais e comunicação à ANPD estão previstos em documento específico – Procedimento IPE-0523-PRO.

O Departamento de Tecnologia e Segurança da Informação e a Equipe de Sistemas Corporativos devem implementar controles técnicos de modo a capacitar o Eldorado na identificação de possíveis violações de dados pessoais em seus ambientes lógicos, possibilitando reportá-las em tempo hábil à ANPD e, se for o caso, aos titulares envolvidos.

É dever dos integrantes do Eldorado e dos parceiros de negócios comunicar o Encarregado de Dados Pessoais, sem demora injustificada, acerca de qualquer incidente de segurança que envolva a violação (ou a tentativa de violação) a dados pessoais do qual venham a ter conhecimento.



Tanto os integrantes do Eldorado quanto os parceiros de negócios devem, na medida de suas responsabilidades e possibilidades, cooperar para a investigação de incidentes de segurança e mitigação de riscos.

Todos os procedimentos relativos a este tópico devem ser documentados pelas partes envolvidas, sob a supervisão do Encarregado pelo Tratamento de Dados Pessoais, conforme estabelecido no Procedimento IPE-0523-PRO.

## **12. MEDIDAS DISCIPLINARES**

O descumprimento desta Política acarretará a aplicação de uma medida disciplinar, conforme estabelecido no Código de Conduta e na Política de Gestão do Programa de Ética e Compliance (IPE-0362-ORG), sem prejuízo da adoção, pelo Eldorado, de medidas judiciais ou administrativas, quando cabíveis.

\*\*\*\*\*