compesa

POLÍTICA

GGR-POL-009-02

Vigência até: 24/10/2025

**Titulo:**

Política de Privacidade e Proteção de Dados Pessoais

**Elaborado/Alterado por:**

GERÊNCIA DE COMPLIANCE GESTÃO DE RISCOS E CONTROLE INTERNO - GGR

**Aprovado por:**

Diretoria Colegiada

## 1. OBJETIVO

Esta Política estabelece as orientações gerais para a proteção de dados pessoais dentro do ambiente corporativo da COMPESA, uma vez que, na execução de suas operações, coleta, manuseia e armazena informações que podem estar relacionadas a pessoas físicas identificadas e/ou identificáveis (“Dados Pessoais”), com vistas a:

- Estar em conformidade com as leis e regulamentações aplicáveis de proteção de Dados Pessoais e seguir as melhores práticas;
- Proteger os direitos dos integrantes, clientes, fornecedores e parceiros contra os riscos de violações de Dados Pessoais;
- Ser transparente com relação aos procedimentos da Companhia no Tratamento de Dados Pessoais; e
- Promover a conscientização em toda a Companhia em relação à proteção de Dados Pessoais e questões de privacidade.

## 2. APLICAÇÃO

Esta Política é aplicável à Compesa e a todos os parceiros que tenham acesso a quaisquer Dados Pessoais detidos por esta Companhia ou em seu nome. Procedimentos adicionais podem ser criados de acordo com exigência da legislação local.

Qualquer legislação aplicável deve prevalecer caso esteja ou venha a estar em conflito com esta Política.

## 3. DEFINIÇÕES

**3.1 Anonimização**: Processo e técnica por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Dado anonimizado não é considerado Dado Pessoal.

**3.2 Consentimento**: Manifestação livre, informada e inequívoca pela qual o Titular concorda com o Tratamento de seus Dados Pessoais para uma finalidade determinada.

**3.3 Controlador**: Pessoa jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.

**3.4 Dado(s) Pessoal(ais)**: Qualquer informação relativa a uma pessoa singular identificada ou identificável, que pode ser identificada, direta ou indiretamente, por referência a um identificador como nome, número de identificação, dados de localização, identificador *on-line* ou a um ou mais fatores específicos a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

**3.5 Dado(s) Pessoal(ais) Sensível(eis)**: Todo Dado Pessoal que pode gerar qualquer tipo de discriminação como, por exemplo, os dados 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.

**3.6 Encarregado de Proteção de Dados ou *Data Protection Officer* (DPO)**: O profissional designado como encarregado formal/oficial de proteção de dados, conforme previsto nas leis de proteção de dados, tais como GDPR e LGPD, para um determinado território. O DPO pode ser um colaborador ou uma pessoa terceirizada.

**3.7 GDPR**: Regulamento (UE) 2016/679 do Parlamento Europeu de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao Tratamento de Dados Pessoais e à livre circulação desses dados e que revoga a Diretiva 95 / 46 / CE (Regulamento Geral de Proteção de Dados).

**3.8 LGPD**: Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de Tratamento de Dados Pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

**3.9 Política de Segurança da Informação**: Diretrizes corporativas globais da Compesa sobre Segurança da Informação, conforme normativo GTI-POL-001/Compesa , que podem ser alteradas periodicamente.

**3.10 Dado pessoal de criança e adolescente:** Dado relativo a pessoas menores de 18 anos.

## 4. RESPONSABILIDADES

**4.1 Gerência de Compliance, Gestão de Riscos e Controle Interno**

Manter atualizado a norma conforme definido pela Lei nº 13.709 (Lei Geral de Proteção de Dados) de 14/08/2018 e suas atualizações;

Verificar o atendimento às definições constantes nesta norma;

**4.2 Demais unidades organizacionais da Compesa**

Atender às determinações inscritas neste documento.

## 5. DETALHAMENTO

**5.1 PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS**

Esta seção descreve os princípios que devem ser observados na coleta, manuseio, armazenamento, divulgação e Tratamento de Dados Pessoais pela Compesa para atender aos padrões de proteção de dados no âmbito corporativo e estar em conformidade com a legislação e regulamentação aplicáveis onde tiver operação ou atividade comercial.

**5.1.1 Legalidade, Transparência e Não Discriminação**

I - A Compesa trata os Dados Pessoais de forma justa, transparente e em conformidade com legislação e regulamentação aplicáveis.

II - A Compesa somente trata Dados Pessoais quando o propósito/finalidade do tratamento se enquadra em uma das hipóteses legais permitidas, abaixo elencadas, sendo certo que os Titulares de Dados devem ser informados sobre a razão e a forma pela qual seus Dados Pessoais estão sendo tratados antes ou durante a coleta:

a) necessidade para a execução de um contrato do qual o Titular dos Dados é parte;

b) exigência decorrente de lei ou regulamento ao qual a Compesa está sujeita;

c) interesse legítimo pelo Tratamento, hipótese na qual tal interesse legítimo será comunicado previamente; e

d) necessidade de prover ao Titular dos Dados o exercício regular de direito em processo judicial, administrativo ou arbitral.

III - Quando o Tratamento de Dados Pessoais não se enquadrar nas hipóteses acima, a Compesa deve obter o Consentimento dos Titulares dos Dados para o Tratamento de seus Dados Pessoais e assegurar que este Consentimento seja obtido de forma específica, livre, inequívoca e informada. A COMPESA deve coletar, armazenar e gerenciar todas as respostas de Consentimento de maneira organizada e acessível para que a comprovação de Consentimento possa ser fornecida quando necessário.

IV - Da mesma forma, o Titular de Dados deve ter a possibilidade de retirar o seu Consentimento a qualquer momento com a mesma facilidade que foi fornecido.

V - Em algumas circunstâncias, a Compesa também pode ser obrigada a tratar Dados Pessoais Sensíveis, envolvendo, mas não se limitando, a:

a) dados relacionados à saúde ou à vida sexual;

b) dados genéticos ou biométricos vinculados a uma pessoa física;

c) dados sobre orientação sexual;

d) dados sobre condenações ou ofensas criminais;

e) dados que evidenciem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas; e

f) dados referentes à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

VI - O Tratamento de Dados Pessoais Sensíveis é proibido, exceto nos casos específicos descritos abaixo, nos quais deverão ser observados padrões de segurança mais robustos do que os empregados aos demais Dados Pessoais:

a) quando for necessário para o cumprimento de obrigação legal ou regulatória;

b) quando for necessário para o exercício regular de direitos a exemplo da defesa ou proposição de ações judiciais, administrativas ou arbitrais;

c) quando for necessário para o cumprimento de obrigações e o exercício de direitos em matéria de emprego, previdência social e proteção social;

d) para proteção à vida ou à incolumidade física do Titular do Dado incluindo dados médicos com fins preventivos e/ou ocupacionais;

e) para fins de promoção ou manutenção de igualdade de oportunidades entre pessoas de origem racial ou étnica diferente; e

f) quando o Titular dos Dados tiver dado o seu Consentimento explícito, de acordo com a legislação e regulamentação aplicáveis.

**5.1.2 Limitação e Adequação da Finalidade**

O Tratamento de Dados Pessoais deve ser realizado de maneira compatível com a finalidade original para a qual os Dados Pessoais foram coletados, não podendo ser coletados com um propósito e utilizados para outro. Quaisquer outras finalidades devem ser compatíveis com a razão original para qual os Dados Pessoais foram coletados.

**5.1.3 Princípio da Necessidade (Minimização dos Dados)**

A Compesa somente pode tratar Dados Pessoais na medida em que seja necessário para atingir um propósito específico. O compartilhamento de Dados Pessoais com outra área ou outra empresa deve considerar este princípio, só podendo ser compartilhados quando tenham um amparo legal adequado.

**5.1.4 Exatidão (Qualidade dos Dados)**

A Compesa deve adotar medidas razoáveis para assegurar que quaisquer Dados Pessoais em sua posse sejam mantidos precisos e atualizados em relação às finalidades para as quais foram coletados, sendo certo que deve ser possibilitado ao Titular do Dado Pessoal a possibilidade de requerer a exclusão ou a correção de dados imprecisos ou desatualizados.

**5.1.5 Retenção e Limitação do Armazenamento de Dados**

A Compesa deve ter conhecimento de suas atividades de Tratamento, dos períodos de retenção estabelecidos e dos processos de revisão periódica, não podendo manter os Dados Pessoais por prazo superior ao necessário para atender as finalidades pretendidas.

**5.1.6 Integridade e Confidencialidade (Livre Acesso, Prevenção e Segurança)**

A Compesa  deve assegurar que medidas técnicas e administrativas apropriadas sejam aplicadas aos Dados Pessoais para protegê-los contra o Tratamento não autorizado ou ilegal, bem como contra a perda acidental, destruição ou danos. O Tratamento de Dados Pessoais também deve garantir a devida confidencialidade. Dentre as medidas técnicas mais comuns, podem ser descritas:

I - Anonimização: os Dados Pessoais são tornados anônimos de tal forma que não mais se referem a uma pessoa direta ou indiretamente identificável. O anonimato tem que ser irreversível;

II - Pseudoanonimização: os Dados Pessoais não mais se relacionam diretamente com uma pessoa identificável (por exemplo, mencionando seu nome), mas não é anônimo porque ainda é possível, com informações adicionais, que são mantidas separadamente, identificar uma pessoa.

**5.1.7 Responsabilização e Prestação de Contas**

A Compesa é responsável e deve demonstrar o cumprimento desta Política, assegurando a implementação de diversas medidas que incluem, mas que não estão limitadas a:

I - Garantia de que os Titulares dos Dados Pessoais possam exercer os seus direitos;

II - Registro de Dados Pessoais, incluindo:

a) registros de atividades de Tratamento de Dados Pessoais com a descrição dos propósitos/finalidades desse Tratamento, os destinatários do compartilhamento dos Dados Pessoais e os prazos pelos quais a Compesa deve retê-los; e

b) registro de incidentes de Dados Pessoais e violações de Dados Pessoais;

III - Garantia de que os Terceiros que sejam Processadores de Dados Pessoais também estejam agindo de acordo com esta Política e com a legislação e regulamentação aplicáveis;

IV - Garantia de que a Compesa, quando requerido, registre junto à Autoridade Supervisora aplicável um Encarregado de Dados ou DPO; e

V - Garantia de que a Compesa esteja cumprindo todas as exigências e solicitações de qualquer Autoridade de Supervisão à qual esteja sujeita.

**5.2 PADRÕES DE SEGURANÇA**

**5.2.1 Importância da Proteção de Dados Pessoais**

A Compesa está comprometida com a implementação dos padrões de Segurança da Informação e com a proteção de Dados Pessoais com vistas a garantir o direito fundamental do indivíduo à autodeterminação da informação.

**5.2.2 Garantir a Segurança dos Dados Pessoais**

A confidencialidade, integridade e disponibilidade, bem como autenticidade, responsabilidade e não-repúdio são objetivos a serem perseguidos para a segurança dos Dados Pessoais.

**5.2.3 Obrigação do Sigilo de Dados Pessoais**

Todos os Integrantes com acesso a Dados Pessoais estão obrigados aos deveres de confidencialidade dos Dados Pessoais mediante a anuência ao Código de Conduta e Integridade, quando do ingresso na Compesa e periodicamente, nos termos da Lei nº 13.303/2016.

**5.2.4 Privacidade de Dados Pessoais por Concepção e por Padrão**

Ao implementar novos processos, procedimentos ou sistemas que envolvam o Tratamento de Dados Pessoais, a Compesa deve adotar medidas para garantir que as regras de Privacidade e Proteção de Dados sejam adotadas desde a fase de concepção até o lançamento/implantação destes projetos.

**5.3 DIREITOS DOS TITULARES DE DADOS PESSOAIS**

A Compesa está comprometida com os direitos dos Titulares de Dados Pessoais, os quais incluem:

I - Informação, no momento em que os Dados Pessoais são fornecidos, sobre como seus Dados Pessoais serão tratados;

II - Informação sobre o Tratamento de seus Dados Pessoais e o acesso aos Dados Pessoais que a Compesa detenha sobre eles;

III - Correção de seus Dados Pessoais se estiverem imprecisos, incorretos ou incompletos;

IV - Exclusão, bloqueio e/ou anonimização de seus Dados Pessoais em determinadas circunstâncias (“direito de ser esquecido”). Isso pode incluir, mas não se limita a, circunstâncias em que não é mais necessário que a Compesa retenha seus Dados Pessoais para os propósitos para os quais foram coletados;

V - Restrição do Tratamento de seus Dados Pessoais em determinadas circunstâncias;

VI - Opor-se ao Tratamento, se não estiver baseado em legítimo interesse;

VII - Retirar o Consentimento a qualquer momento, se o Tratamento dos Dados Pessoais se basear no Consentimento do indivíduo para um propósito específico;

VIII - Portabilidade dos Dados Pessoais a outro fornecedor de serviço ou produto mediante requisição expressa em determinadas circunstâncias;

IX - Revisão das decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais; e

X - Apresentação de queixa à Compesa ou à Autoridade de Proteção de Dados aplicável, se o Titular dos Dados Pessoais tiver motivos para supor que qualquer um de seus direitos de proteção de Dados Pessoais tenha sido violado.

**5.4 TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES**

O tratamento dos dados pessoais de crianças e adolescentes deve se dar no melhor interesse de seus titulares.

I - Os dados de crianças (menores de 12 anos) normalmente são tratados com o consentimento de, ao menos, um de seus responsáveis legais, com exceção das situações legais em que o consentimento não é exigido, como, por exemplo, na execução de serviço público;

II - A informação sobre o tratamento de dados pessoais sensíveis ou referentes a crianças ou adolescentes estará disponível em linguagem clara e simples, com concisão, transparência, inteligibilidade e acessibilidade, na forma da lei e de acordo com as regras do regime de tramitação sob segredo de Justiça.

**5.5 PRESTADORES DE SERVIÇOS TERCEIRIZADOS**

Os prestadores de serviços terceirizados que tratem Dados Pessoais sob as instruções da Compesa estão sujeitos às obrigações impostas aos Processadores de acordo com a legislação e regulamentação de proteção de Dados Pessoais aplicáveis. A Compesa deve assegurar que no contrato de prestação de serviço sejam contempladas as cláusulas de privacidade que exijam que o Processador de Dados terceirizado implemente medidas de segurança, bem como controles técnicos e administrativos apropriados para garantir a confidencialidade e segurança dos Dados Pessoais e especifiquem que o Processador está autorizado a tratar Dados Pessoais apenas quando seja formalmente solicitado pela Compesa .

### 5.6 GERENCIAMENTO DE VIOLAÇÃO DE DADOS

I - Todos os incidentes e potenciais violações de dados devem ser reportadas à **Gerência de Compliance, Gestão de Riscos e Controle Interno (GGR)** da Compesa. Todos os colaboradores devem estar cientes de sua responsabilidade pessoal de encaminhar e escalonar possíveis problemas, bem como de denunciar violações ou suspeitas de violações de Dados Pessoais assim que as identificarem. No momento em que um incidente ou violação real for descoberto, é essencial que os incidentes sejam informados e formalizados de forma tempestiva.

II - Violações de dados incluem, mas não se limitam a, qualquer perda, exclusão, roubo ou acesso não autorizado de dados pessoais controlados ou tratados pela Compesa.

III - O registro e o tratamento de incidentes de segurança da informação que envolvam violação de dados pessoais devem se tratados conforme Plano de Resposta à Incidentes de Dados, anexo I.

IV - A avaliação dos riscos inerentes ao tratamento de dados pessoais bem como as medidas para mitigação dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares dos dados estão descritos em documento próprio intitulado Relatório de Impacto à Proteção dos Dados Pessoais (RIPD), anexo II.

### 5.7 AUDITORIAS DE PROTEÇÃO DE DADOS

I - A Compesa deve garantir que existam revisões periódicas a fim de confirmar que as iniciativas de Privacidade, seu sistema, medidas, processos, precauções e outras atividades, incluindo o gerenciamento de proteção de Dados Pessoais, são efetivamente implementados e mantidos e estão em conformidade com a legislação e regulamentação aplicáveis.

II - Adicionalmente e, conforme previsto no Normativo AUD-NI-001/Compesa, o tema deve ser avaliado com a devida periodicidade e de acordo com os riscos existentes. Caso os riscos sejam relevantes, a Auditoria Interna (AUD) da Compesa deverá incluir revisão específica independente no plano anual de auditoria interna.

## 6. INSTRUMENTOS NORMATIVOS RELACIONADOS

- GGR-POL-008: Política de Gestão de Riscos
- GTI-POL-001: Política de Segurança da Informação
- GGR-NI-003: Norma Interna de Gestão de Riscos
- AUD-NI-001: Norma de Auditoria Interna
- Código de Conduta e Integridade COMPESA

## 7. REFERÊNCIAS


- Constituição da República Federativa do Brasil de 1988;
- Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 13.303, de 30 de junho de 2016: Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;
- Regulamento Geral sobre a Proteção de Dados 2016/679 (GDPR).


## 8. HISTÓRICO DE ALTERAÇÕES

| Nº da Versão | Data | Natureza da Revisão e/ou Alteração | RD vinculada |
|---|---|---|---|
| 1 | 27/01/2021 | Emissão inicial | RD 026/2020 |
| 2 | 25/10/2023 | Atualização | RD 015/2023 |

## ANEXOS

**ANEXO 1 - Anexo I - Plano de Resposta a Incidentes de Segurança e Privacidade**
Plano de Resposta revisado e atualizado em abril/2023

**ANEXO 2 - Anexo II - Relatório de Impacto à Proteção de Dados - RIPD**
Relatório com os riscos revisado em abril/2023