

PL-0004 – POLÍTICA DE GOVERNANÇA DE DADOS PESSOAIS

1. OBJETIVO

A Política de Governança de Dados Pessoais da Copagaz Distribuidora de Gás S.A. e da Liquegás Distribuidora S.A., conjuntamente denominadas “Companhia”, tem como objetivo estabelecer os princípios e as diretrizes que nortearão a Companhia na gestão e Tratamento de dados pessoais.

2. APLICAÇÃO E ABRANGÊNCIA

Esta Política deve ser observada por todos os administradores, colaboradores da Companhia, membros de comitês de assessoramento ao Conselho de Administração e terceiros, como também a quaisquer outros indivíduos que atuem na condução ou representação dos negócios da Companhia, devendo ser observada em todas as interações mantidas com clientes, parceiros, fornecedores e demais públicos de relacionamento.

3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.
Código de Conduta Ética

4. DESCRIÇÃO

Esta Política apresenta as diretrizes da proteção aos Dados Pessoais, a importância da adoção das melhores práticas, reforçando a cultura interna e priorizando as ações necessárias conforme o negócio.

4.1. Princípios de privacidade e proteção de Dados Pessoais

4.1.1. O Tratamento de Dados Pessoais deve ser regido pelos seguintes princípios:

a) Finalidade

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 diversas.

b) Adequação

Os Dados Pessoais devem ser tratados de modo adequado e pertinente às suas finalidades de uso.

c) Necessidade e proporcionalidade

O Tratamento dos Dados Pessoais deve ser proporcional aos objetivos do negócio, não sendo feito tratamento de tipos de Dados Pessoais que não sejam necessários e proporcionais a eles.

d) Livre acesso

Assegurar aos titulares a consulta facilitada e gratuita sobre a forma e a duração do Tratamento de seus Dados Pessoais.

e) Qualidade dos dados

Assegurar aos titulares, a exatidão, clareza, relevância e atualização dos Dados Pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

f) Transparência

Assegurar que os titulares tenham informações claras, precisas e facilmente acessíveis sobre o Tratamento de seus Dados Pessoais, observados os segredos comercial e industrial.

Antes de realizar o Tratamento de Dados Pessoais, deve estar disponível ao titular dos Dados Pessoais informação clara, concisa, inteligível, de fácil acesso e de fácil compreensão sobre a coleta, finalidade, armazenamento, compartilhamento e descarte de seus Dados Pessoais.

g) Segurança

O tratamento deve ser realizado de modo a assegurar a proteção e segurança dos Dados Pessoais, incluindo a proteção contra o tratamento não autorizado ou ilícito, perda, destruição ou dano acidental, devendo a Companhia adotar medidas técnicas e organizacionais necessárias para salvaguardar a integridade, confidencialidade e disponibilidade dos Dados Pessoais.

h) Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais.

i) Não discriminação

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

j) Responsabilização e prestação de contas:

Demonstração da adoção de medidas eficazes que comprovem a observância e o cumprimento das normas de proteção de Dados Pessoais.

4.2. Bases legais para Tratamento de Dados Pessoais

4.2.1. O Tratamento dos Dados Pessoais deve ser realizado de modo lícito, justo e transparente com relação ao titular:

a) Dados Pessoais

O Tratamento de Dados Pessoais somente é permitido e, portanto, está legitimado:

I. Com o consentimento do titular dos Dados Pessoais, conforme detalhado no item 4. É vedado o Tratamento de Dados Pessoais mediante Vício de Consentimento;

II. Em caso do cumprimento de uma obrigação legal ou regulatória pela Companhia;

III. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

IV. Para a realização de estudos por instituto, órgão de pesquisa ou empresas especializadas, garantida, sempre que possível, a anonimização dos Dados Pessoais;

V. Quando os Dados Pessoais são necessários para a execução/cumprimento de um contrato com o titular ou os Dados Pessoais do titular são necessários para procedimentos preliminares para se firmar o contrato;

VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, prezando sempre pelo pedido de segredo de justiça quando envolver Dado Pessoal;

VII. Para a proteção da vida ou da segurança física da pessoa a quem os Dados Pessoais se referem;

VIII. Para proteção da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX. Por interesse legítimo da Companhia ou de terceiros, sendo obrigatória a confecção de relatório de impacto à proteção de Dados Pessoais; e/ou

X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

b) Dados Pessoais Sensíveis

O Tratamento de Dados Pessoais Sensíveis, de acordo com a criticidade do processo de negócio, deve ser precedido de relatório de impacto à proteção de Dados Pessoais.

As hipóteses legais de Tratamento de Dados Pessoais Sensíveis, conforme ordenamento jurídico brasileiro vigente são:

I. Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; ou

II. Sem o fornecimento de consentimento, quando for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos Dados Pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

e) proteção da vida ou da incolumidade física do titular ou de terceiros;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais.

4.3. Diretrizes gerais para tratamento de Dados Pessoais

4.3.1. O Tratamento de Dados Pessoais significa toda e qualquer operação realizada pela Companhia com Dados Pessoais, a exemplo de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração entre outras operações possíveis.

4.3.2. O Tratamento de Dados Pessoais deve ser realizado de acordo com os princípios do item 4.1 desta Política:

a) Ciclo de vida do Dado Pessoal

Todo o ciclo de vida do Dado Pessoal na Companhia deverá estar de acordo com as diretrizes desta Política, bem como diretrizes quanto à transferência internacional indicadas em procedimento próprio.

b) Contratos

A Companhia na figura de Controlador do Dado Pessoal, sempre que fizer uso de um Operador, deve estabelecer contrato tendo em vista as regulamentações relacionadas à privacidade e proteção de Dados Pessoais vigentes no país onde ocorrerá o Tratamento dos Dados Pessoais.

c) Relatório de Impacto a Proteção dos Dados Pessoais (RIPD)

O relatório de Impacto à Proteção de Dados Pessoais visa a descrição dos processos de Tratamento de Dados Pessoais e as medidas e mecanismos empregados para mitigar esses riscos pela Companhia.

Todo Tratamento de Dados Pessoais tendo como base legal o legítimo interesse deve ser precedido de relatório de impacto à proteção de Dados Pessoais, conforme procedimento específico.

O relatório de impacto à proteção de Dados Pessoais deve ser elaborado pelo encarregado pelo Tratamento de dados pessoais, com envolvimento das Gerências necessárias para entendimento da elaboração deste relatório, conforme procedimento específico e, também, de acordo com as diretrizes de procedimento próprio.

d) Segurança da Informação

Durante todo o ciclo de vida do Dado Pessoal, devem ser observadas as diretrizes de segurança existentes quanto a segurança da informação na Companhia.

e) Decisões automatizadas

As Gerências devem listar os processos sob sua responsabilidade que envolvem decisões automatizadas baseada no Tratamento de Dados Pessoais que ocorrem em sua Gerência.

Toda decisão automatizada que envolve o Tratamento de Dados Pessoais deve ser formalizada internamente com informações claras e adequadas, disponíveis aos titulares dos Dados Pessoais, quanto aos:

- Critérios utilizados para tomada de decisão automatizada;
- Procedimentos utilizados para tomada de decisão automatizada.

O titular dos Dados Pessoais tem o direito de solicitar a revisão de tomada de decisão baseada em Tratamento automatizado dos Dados Pessoais, tendo o acesso aos critérios e procedimentos, não sendo exigido que esta revisão seja realizada por pessoa natural.

f) Legítimo interesse

O legítimo interesse deverá ser previamente analisado e validado junto a área de Riscos e *Compliance* (Encarregado da Proteção de Dados Pessoais) conforme normativos específicos, levando em consideração a proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem:

- Fazendo coleta dos dados estritamente necessários para a finalidade pretendida;
- Garantindo total transparência ao titular quando o Tratamento dos Dados Pessoais estiver utilizando o legítimo interesse como base; e
- Elaborando Relatório de Impacto à Proteção de Dados Pessoais (RIPD) conforme orientação do item 4.3.2 “c” para as atividades cuja base legal para tratamento seja legítimo interesse.

g) Respostas às solicitações e requisições dos titulares

As diretrizes de procedimentos de resposta às requisições dos titulares dos Dados Pessoais serão regidas por procedimento específico, no tocante a:

- Resposta a requisição do titular dos Dados Pessoais;
- Acesso aos Dados Pessoais pelo titular dos Dados Pessoais;
- Apagamento e/ou bloqueio de Tratamento dos Dados Pessoais por requisição do titular dos Dados Pessoais;
- Resposta a autoridade fiscalizadora;
- Resposta a autoridade judicial.

h) Violações de Dados Pessoais

Os procedimentos relativos a violações de Dados Pessoais devem ser regidos por normativos internos específicos.

A Gerência Executiva de TI deve implementar controles técnicos de modo a capacitar a Companhia quanto a possíveis violações de Dados Pessoais em seus ambientes tecnológicos, possibilitando reportar estas em tempo hábil à ANPD.

Os Colaboradores ou prestadores de serviço têm o dever de notificar a Gerência de Riscos e *Compliance*, sem demora injustificada, acerca de qualquer violação ou tentativa de Violação de Dados Pessoais da qual tenham conhecimento. O Encarregado de dados (Riscos e *Compliance*) sempre reportará incidente à Gerência Executiva de TI, no que tange aos aspectos de segurança da informação.

Os Colaboradores ou prestadores de serviço devem cooperar para a investigação e mitigação de incidentes de Violação de Dados Pessoais.

Todos os procedimentos realizados neste item devem ser documentados pelas partes envolvidas, sob a supervisão do Encarregado pelo Tratamento de Dados Pessoais.

i) Dados de Saúde

O Tratamento de Dados de Saúde deverá, obrigatoriamente, permitir ao titular o direito a portabilidade dos seus dados, quando solicitada, ou as transações financeiras e administrativas resultantes do uso e da prestação dos serviços, nos termos regulamentados pela ANPD.

Os Dados de Saúde poderão ser compartilhados pela Companhia com terceiros se for realizado, exclusivamente: De acordo com o consentimento do titular

- Para cumprimento de obrigação legal ou regulatória pela Companhia
- Para o exercício regular de direitos da Companhia, inclusive em contrato e em processo judicial, administrativo e arbitral
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

Quando houver o compartilhamento de dados de saúde com terceiros, especialmente no caso de operadores de planos de saúde e de outros provedores de benefícios, o compartilhamento levará em consideração os interesses dos titulares, exclusivamente para:

- prestação de serviços de saúde;
- assistência farmacêutica;
- assistência à saúde, inclusive saúde ocupacional;
- serviços auxiliares de diagnose;
- serviços de terapia;
- cálculo atuarial; e/ou
- estudos para definição de modelo de plano de saúde.

4.4. Atribuições e Responsabilidades

4.4.1. Gerência de Riscos e Compliance

- a) Elaborar e/ou revisar os procedimentos internos relativos à proteção de Dados Pessoais;
- b) Organizar e/ou ministrar treinamentos sobre proteção de Dados Pessoais aos colaboradores ou prestadores de serviço, promovendo a cultura de proteção de Dados Pessoais na Companhia;

- c) Apoiar na análise de questões relacionadas à proteção de Dados Pessoais em contratos que envolvam Tratamento de Dados Pessoais, após primeira avaliação da Diretoria Jurídica, seguindo o framework legal específico aplicável a cada situação em suas particularidades;
- d) Apoiar investigações para apuração de responsabilidade dos envolvidos em violações de Dados Pessoais e auxiliar na definição de aplicação das penalidades internas, quando necessário;
- e) Avaliar e auxiliar na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais;
- f) Manter mapeamento de fluxos de Dados Pessoais atualizado;
- g) Monitorar o cumprimento da Tabela de Temporalidade, a ser definida em normativo específico;
- h) Desenvolver plano de análise e resposta às violações de Dados Pessoais que identifique o tipo de violação, o número de registros afetados, quais registros foram afetados e as categorias de Dados Pessoais envolvidas, as notificações apropriadas e plano de mitigação dos efeitos da violação;
- i) Receber as requisições dos titulares dos Dados Pessoais sobre privacidade e proteção de Dados Pessoais, bem como as comunicações da ANPD;
- j) Verificar a adequação das práticas e políticas da Companhia no que se refere à transferência internacional de Dados Pessoais e ao manejo de Dados Pessoais sensíveis;
- k) Assegurar a divulgação e a disponibilidade dos documentos que compõem esta Política e outras políticas internas para proteção de Dados Pessoais na Companhia; e
- l) Definir, em conjunto com as áreas técnicas, as “políticas de uso de site”, “políticas de cookies” e “termos de uso” – Documentos que embora possam ser intitulados como “políticas”, de fato, referem-se a documentos técnicos que funcionam como avisos legais aos usuários dos websites da Companhia;

4.4.2. Gerência Executiva de TI

- a) Analisar os aspectos técnicos de todo e qualquer produto ou serviço de terceiros que a Companhia esteja considerando contratar para processar ou armazenar Dados Pessoais (exemplos: nuvem, hardware, equipamentos de rede); e
- b) Atuar de forma coordenada com a Área de Riscos e *Compliance* (Encarregado pelo Tratamento de Dados Pessoais) para viabilizar a implementação de procedimentos e rotinas necessárias para o Tratamento de Dados Pessoais.

4.4.3. Diretoria Jurídica

- a) Participar previamente dos processos de contratação e aquisição de produtos e serviços da Companhia, validando as minutas contratuais como forma de garantir aderência aos controles de proteção de Dados Pessoais aplicáveis;
- b) Apoiar a Gerência de Riscos e *Compliance* na elaboração de comunicados oficiais de repostas à ANPD; e
- c) Fornecer orientação legal quanto às medidas a serem tomadas nas ocorrências de incidentes de Violação de Dados Pessoais.

4.4.4. Diretoria de RH

- a) Assegurar que os colaboradores que tratam Dados Pessoais tenham assinado compromissos de confidencialidade que incluam disposições específicas para o Tratamento de Dados Pessoais; e
- b) Estipular controles de proteção de Dados Pessoais especificamente relacionados aos processos de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões).

4.4.5. Marketing

- a) Elaborar, com o apoio da Gerência de Riscos e *Compliance*, campanhas de conscientização e materiais de divulgação e alerta relacionados à proteção de Dados Pessoais;
- b) Analisar e aprovar o formato das comunicações relacionadas à proteção de Dados Pessoais;
- c) Responder, seguindo as orientações da Gerência de Riscos e *Compliance*, eventuais questionamentos de veículos de imprensa;
- d) Submeter à análise da Gerência de Riscos e *Compliance* textos e comunicados sobre privacidade e proteção de Dados Pessoais, antes de sua publicação; e
- e) Submeter à análise da Gerência de Riscos e *Compliance* todas as ações promovidas por esta gerência que envolvam o Tratamento de Dados Pessoais, como por exemplo, promoções, campanhas de incentivo, feiras entre outros, antes de sua formalização na Companhia.

4.4.6. Lideranças.

- a) Cumprir, fazer cumprir e gerenciar o cumprimento desta Política e demais documentos complementares por parte de seus colaboradores ou prestadores de serviço;

b) Assegurar que qualquer Dado Pessoal só poderá ser recebido, tratado, excluído ou compartilhado por sua Gerência mediante notificação à Gerência de Riscos e *Compliance*;

c) Submeter à análise do encarregado de dados todo novo processo, incluindo novas aplicações, contratações, serviços, produtos, campanhas, dentre outros, onde houver Tratamento de Dados Pessoais;

d) Garantir a observação desta Política e da legislação competente pelos parceiros de negócio que recebam Dados Pessoais enviados por sua gerência, devendo:

- Obter documentos (procedimentos internos de segurança da informação, treinamento aplicado aos colaboradores ou prestadores de serviços que manuseiam os Dados Pessoais, lista de controle de acesso, por exemplo) e garantias (acordo de confidencialidade assinado pelos colaboradores, cláusulas contratuais, dentre outras) do parceiro de negócio que confirmem a segurança no manuseio dos Dados Pessoais sob responsabilidade da Companhia;
- Requerer, por meio de contrato, que o parceiro de negócios obtenha aprovação prévia e por escrito da Companhia antes de qualquer subcontratação para fins de Tratamento de Dados Pessoais sob responsabilidade da Companhia, independente de previsão legal nesse sentido; e
- Requerer, por meio de contrato, que o parceiro de negócios se abstenha de utilizar os Dados Pessoais sob responsabilidade da Companhia para qualquer outro propósito, e que, após concluído o objeto do contrato, que sejam devolvidos e/ou eliminados todos os Dados Pessoais enviados ou compartilhados pela Companhia ao parceiro.

e) Preparar e manter atualizada uma lista com todas as categorias de Dados Pessoais tratados em sua Gerência, e submeter essa lista à Gerência de Riscos e *Compliance*;

f) Zelar pelo cumprimento da Tabela de Temporalidade vigente, conforme normativo específico;

g) Assegurar que os Dados Pessoais são coletados, usados ou gerenciados apenas por colaboradores ou prestadores de serviços autorizados, devendo:

- Classificar os Dados Pessoais tratados em sua gerência de acordo com as diretrizes da Companhia;
- Aprovar acesso aos colaboradores ou prestadores de serviço diretamente envolvidos nas atividades que demandam os Dados Pessoais;
- Assegurar que os colaboradores ou prestadores de serviço sob sua supervisão realizem treinamentos em proteção de Dados Pessoais e conheçam as políticas internas da Companhia;

- Atuar em parceria com as demais Gerências da Companhia para identificar as vulnerabilidades e ameaças à proteção de Dados Pessoais nos processos e atividades de sua responsabilidade; e
- Assegurar que os Dados Pessoais sob a sua responsabilidade sejam utilizados com cuidado e de acordo com as orientações legais aplicáveis;

h) Ao identificar violações de Dados Pessoais ou qualquer ação duvidosa, comunicar a Gerência de Riscos e *Compliance* imediatamente, considerando os meios de comunicação disponíveis e

i) Coletar e manter registros das atividades de Tratamento de Dados Pessoais dos processos sob sua gestão, desde evidências que comprovem o consentimento dos titulares dos Dados Pessoais (logs de consentimento, por exemplo) até registro de utilização, compartilhamento, exclusão e outros, pelo período legal exigido conforme a Tabela de Temporalidade prevista em normativo específico.

4.4.7. Demais Colaboradores

a) Cumprir as diretrizes deste padrão e seus documentos complementares;

b) Tratar os Dados Pessoais sob responsabilidade da Companhia somente para fins autorizados, de forma ética e legal, respeitando os direitos do titular dos Dados Pessoais e de acordo com as orientações desta Política, demais instrumentos regulamentares relacionados à proteção de Dados Pessoais e da legislação aplicável; e

c) Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e Legalidade dos Dados Pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente estes Dados Pessoais, em qualquer local ou mídia, inclusive na Internet, de acordo com as diretrizes de proteção e Tratamento das informações definidos pela Companhia.

4.4.8. Violações desta Política

Todos os colaboradores têm o dever de reportar prontamente qualquer violação ou suspeita de violação da presente Política ao Canal de Denúncias da Companhia, através do [link www.aloetica.com.br/copaenergia](http://www.aloetica.com.br/copaenergia) ou pelo telefone **0800 795 1509**.

Em caso de violação às diretrizes contidas nessa Política, serão aplicadas medidas disciplinares previstas no Código de Conduta Ética da Companhia e, em sendo necessário, os fatos serão reportados às autoridades competentes conforme a avaliação do Comitê de Ética na forma do seu Regimento Interno.

5. DEFINIÇÕES

Agente de Tratamento: controlador e operador.

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da Lei de Proteção de Dados Pessoais aplicável.

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.

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

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

Dado anonimizado: dado que não identifica de forma direta ou indireta um titular dos Dados Pessoais, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu Tratamento.

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 física.

Dados de Saúde: dados sensíveis que permitem inferir informações referentes à saúde do titular.

Demais Colaboradores: empregados próprios, empregados de empresas prestadoras de serviços, temporários, estagiários e aprendizes.

Legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do ordenamento jurídico em vigor.

Liderança: Administradores: incluindo CEO, Vices Presidentes e Diretores e Gestores: incluindo Gerentes Executivos, Gerentes Corporativos e Supervisores.

Operador: pessoa física ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do controlador.

Relatório de Impacto à Proteção de Dados Pessoais: 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.

Requisições do titular dos Dados Pessoais: requisição do titular dos Dados Pessoais acerca de seus direitos estabelecidos em lei e relativos ao Tratamento dos seus Dados Pessoais.

Tabela de Temporalidade: instrumento que lista os tipos de registros relacionados à Dados Pessoais em formato físico ou lógico, e por quanto tempo devem ser mantidos, visando estabelecer e documentar períodos de retenção padrão para diferentes categorias de Dados Pessoais.

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.

Vício de Consentimento: possibilidade de que o consentimento para o Tratamento de Dados Pessoais não tenha sido coletado por vontade livre e espontânea do titular, a exemplo de uso de força para coleta do consentimento ou medidas que induzam o usuário ao erro no momento de fornecer consentimento (ex.: coleta de dados do titular que não informados ao titular, mas tratados com base legal de consentimento).

Violação de Dados Pessoais: destruição, perda, alteração, divulgação acidental ou ilegal, não autorizada ou acesso a Dados Pessoais transmitidos, armazenados ou de outra forma processados, resultante de incidente de segurança.

6. ANEXOS

Não aplicável.

Aprovação: PD.CAC-CAC_021/2021, realizada em 16/12/2021.