

**PLANO
DE
GOVERNANÇA
DE
DADOS
PESSOAIS**

PLANO DE GOVERNANÇA DE DADOS PESSOAIS

1. INTRODUÇÃO

A LCL Administração e Serviços Ltda., empresa prestadora de Serviços Comerciais e de Engenharia de Saneamento, Facilities e Consultoria em Gestão de Segurança Privada, pauta sua atuação em:

MISSÃO: “Criar soluções inteligentes, tecnológicas e personalizadas que agreguem valor aos negócios dos clientes”.

VISÃO: “Ser uma empresa reconhecida pela qualidade, inovação e foco no atendimento aos clientes”.

VALORES: Transparência e Integridade, Investimento no Capital Humano, Pesquisa, Inovação e Melhoria Contínua, Foco no Cliente e nos Resultados

Com a edição da Lei Federal nº 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre a proteção de dados pessoais e altera o Marco Civil da Internet, fez-se necessária a adequação da Empresa à legislação, de forma a proteger os dados pessoais de seus colaboradores, prestadores de serviços e clientes.

Assim, a LCL elaborou o seu Plano de Governança de Dados Pessoais que contempla as regras de boas práticas de governança com procedimentos, normas de segurança, ações educativas e mitigação de riscos no tratamento de dados pessoais. O Plano de Governança de Dados Pessoais, alinhado com a missão, a visão e os valores, foi aprovado pela Diretoria da LCL em 02/01/2024, o que reforça o seu comprometimento com as melhores práticas de governança corporativa.

2. OBJETIVO

O Plano de Governança de Dados Pessoais visa demonstrar para a sociedade a forma como a Empresa está gerindo os dados pessoais sob sua responsabilidade.

2.1 Público Alvo

Este Plano aplica-se aos seus colaboradores, prestadores de serviços e usuários.

3. DEFINIÇÕES

- a) **Dados Pessoais:** informações relacionadas a pessoa natural identificada ou identificável.
- b) **Dados Pessoais Sensíveis:** dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural.
- c) **Dados Anonimizados:** dados relativos a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- d) **Banco de Dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- e) **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.
- f) **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- g) **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- h) **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.
- i) **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- j) **Transferência Internacional de Dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
- k) **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

l) Relatório de Impacto à Proteção de Dados Pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

m) Autoridade Nacional de Proteção de Dados: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

4. REFERÊNCIAS

4.1 Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD);

4.2 Política de Privacidade da COPASA MG;

4.3 Política de Proteção de Dados Pessoais da COPASA MG.

5. DESCRITIVO

5.1 Fundamentos da Proteção de Dados Pessoais

A proteção de dados pessoais tem como fundamentos:

- a) o respeito à privacidade;
- b) a autodeterminação informativa;
- c) a liberdade de expressão, de informação, de comunicação e de opinião;
- d) a inviolabilidade da intimidade, da honra e da imagem;
- e) o desenvolvimento econômico e tecnológico e a inovação;
- f) a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

5.2 Requisitos para o Tratamento de Dados Pessoais

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- a) mediante o fornecimento de consentimento pelo titular;
- b) para o cumprimento de obrigação legal ou regulatória pelo controlador;

- c) 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, observadas as disposições do Capítulo IV da Lei Federal nº 13.709/18;
- d) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- e) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- f) para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- g) para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- h) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- i) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- j) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
- k) A LCL utiliza os dados pessoais de seus clientes, prestadores de serviços e empregados para o cumprimento de obrigação legal ou regulatória, em conformidade, portanto, com as disposições da Lei Federal nº 13.709/18.

5.3 Agentes de Tratamento, encarregado, titular e Autoridade Nacional de Proteção de Dados e Comissão de Proteção de Dados Pessoais

Nos termos da Lei Federal nº 13.709/18 são considerados agentes de tratamento as figuras do controlador e operador.

O “Controlador” é a própria Diretoria, a quem compete as decisões referentes ao tratamento de dados pessoais e que, por meio dos seus poderes e atribuições, delega as ações necessárias para a operacionalização da Política de Proteção de Dados Pessoais.

O “Encarregado” é a pessoa designada pela Diretoria para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Os titulares são as pessoas naturais a quem se referem os dados pessoais que são objeto de tratamento, ou seja, usuários da Empresa, seus empregados e prestadores de serviços.

A Comissão de Proteção de Dados Pessoais é composta por empregados designados para tratar de assuntos relevantes sobre a proteção de dados pessoais.

Por fim, a Autoridade Nacional de Proteção de Dados é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da legislação.

5.4 Uso Compartilhado

A LCL, poderá compartilhar os dados pessoais que tiver acesso com municípios, Estados, União e órgãos ou entidades da administração direta e indireta.

Para o compartilhamento destes dados deverão ser respeitadas as seguintes condições:

- a) Solicitação formal do órgão ou entidade, apontando as justificativas e a previsão legal para o compartilhamento de dados pessoais;
- b) Celebrar contratos, convênios ou instrumentos congêneres;
- c) Assinatura do Termo de Confidencialidade por aqueles que tiverem acesso a algum dado pessoal que esteja sob a responsabilidade da LCL.

5.5 CONTRATAÇÕES

Os contratos celebrados pela LCL trazem a obrigatoriedade de observância, pelas empresas contratadas, da Lei Federal nº 13.709/18.

6. MEDIDAS DE COMPLIANCE PARA PROTEÇÃO DE DADOS PESSOAIS

São instrumentos que contêm regras de boas práticas de governança que estabelecem procedimentos, normas de segurança, ações educativas e mitigação de riscos no tratamento de dados pessoais:

6.1 Relatório de Impacto à Proteção de Dados Pessoais

O Relatório de Impacto à Proteção de Dados Pessoais é o documento interno da LCL que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

6.2 Políticas

6.2.1 Política de Privacidade

A Política de Privacidade visa proteger os clientes que disponibilizam seus dados pessoais nos sistemas informatizados e que utilizam as aplicações da Empresa.

6.2.2 Política de Proteção de Dados Pessoais

A Política de Proteção de Dados Pessoais, estabelece diretrizes para uniformizar as ações da LCL no que concerne ao tratamento de dados pessoais em seus processos e a proteção desses dados, além de disseminar a cultura de segurança dessas informações em consonância com os seguintes princípios: legalidade, lealdade, transparência, integridade e confidencialidade.

6.3 Plano de Comunicação - Incidente de Segurança

O Plano de Comunicação da LCL estabelece os processos que devem ser utilizados quando da detecção de incidentes de segurança e devem levar em consideração a ameaça em si e o quão sensível são os dados objeto do incidente, nos termos do artigo 46 e seguintes da Lei Federal nº 13.709/18.

Os órgãos fiscalizadores, tais como a Autoridade Nacional, Procon, ARSAE, dentre outros, bem como a imprensa, deverão ser comunicados sobre incidente de segurança que acarrete risco ou dano a clientes, prestadores de serviços, fornecedores ou colaboradores.

7. TREINAMENTO

O Encarregado tem a responsabilidade de promover a comunicação e treinar periodicamente os colaboradores próprios ou terceirizados sobre as boas práticas para a proteção de dados pessoais sob responsabilidade da LCL.

Todos os empregados da LCL receberam e comprometeram-se a cumprir as Políticas de Privacidade e de Proteção de Dados Pessoais.

A LCL se compromete a orientar e fornecer treinamento sobre proteção de dados pessoais para os prestadores de serviços que atuam em seu nome.

8. MONITORAMENTO E TRATAMENTO

É de responsabilidade do Encarregado verificar os resultados alcançados com a implantação do Plano de Governança de Dados. O resultado desse monitoramento será reportado periodicamente à Diretoria, que acompanhará as medidas relacionadas à proteção de dados pessoais.

Elaborado	Aprovado
Pedro Henrique Fortes	Anderson Lara