Política

PDD.01.001

Política de Privacidade e Proteção de Dados

Rev. 02

	Nome	Data
Elaboração	Luana Silva de Oliveira	11/02/2025
Aprovação	Denise Monteiro da Rocha	26/02/2025
Homologação	Fábio Augusto Otaciano Batista	12/03/2025

Índice

1. Introdução e Objetivo 2
2. Aplicação e Alcance 2
3. Referências internas e externas 2
   3.1. Normativos Internos: 2
   3.2. Normativos Externos: 2
4. Definições 2
5. Princípios e Diretrizes 3
6. Coleta, Armazenamento e Tratamento de Dados 4
7. Direitos dos Titulares 5
8. Tratamento de Dados Pessoais e Sensíveis 6
9. Tratamento de Dados Pessoais nas Mídias Digitais 6
10. Resposta a Incidentes e Violações 6
    10.1. Medidas Preventivas e Monitoramento 6
    10.2. Plano de Ação e Resposta a Incidentes 7
    10.3. Comunicação e Transparência 7
11. Papéis e Responsabilidades 7
    11.1. Comitê RiskCo 7
    11.2. Encarregado de Proteção de Dados (DPO) 8
    11.3. Comitê de Governança de Dados (CGD) 8
    11.4. Tecnologia da Informação (TI) 9
    11.5. Usuários 9
12. Sanções 9
    12.1. Sanções para Colaboradores da CMOC Brasil 9
    12.2. Sanções para Colaboradores de Terceiros Contratados 9
    12.3. Responsabilidade de Terceiros no Tratamento de Dados 10
13. Confidencialidade dessa Política 10

Revisão	Alterações
00	Publicação Inicial.
01	Alteração dos responsáveis pela elaboração e aprovação
02	Revisão Geral

Cópia não controlada

1. Introdução e Objetivo

A CMOC Brasil estabelece sua Política de Privacidade e Proteção de Dados (PPPD) como parte do seu sistema de gestão corporativa, garantindo conformidade com a Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/2018, boas práticas e normas internacionais reconhecidas. Essa política define diretrizes para avaliação de riscos, resposta a incidentes, responsabilidades e sanções relacionadas ao tratamento de dados pessoais e sensíveis, assegurando os direitos dos titulares.

O objetivo principal é estabelecer boas práticas de governança de segurança e privacidade de informação, promovendo conscientização e educação dos colaboradores e gestores quanto à proteção de dados.

2. Aplicação e Alcance

Essa política aplica-se a gestores, colaboradores, terceiros, clientes, fornecedores e parceiros da CMOC Brasil, incluindo tanto pessoas físicas quanto jurídicas.

A CMOC Brasil, na qualidade de controladora de dados, estabelece que esta política se aplica a qualquer operação de tratamento de dados pessoais, independentemente do meio ou local onde estejam armazenados, desde que:

a) O tratamento ocorra em território nacional;
b) Envolva oferta de bens ou serviços ou tratamento de dados de indivíduos localizados no Brasil;
c) Os dados tenham sido coletados no Brasil.

3. Referências internas e externas

Essa política interna considera aspectos e diretrizes de outras normativas relacionadas à segurança e privacidade de dados e aos direitos individuais, principalmente àquelas relacionadas:

3.1. Normativos Internos:

a. Plano de Ação, Comunicação e de Resposta a Incidentes (PDD.01.003)
b. Declaração da Política de Segurança da Informação (STI.01.033)
c. Gestão de Identidade e Acessos (STI.01.063)
d. Código de Conduta (CODCONDUTA)
e. Integridade Empresarial CMOC Brasil (GOV.01.004)
f. Book de Governança (GOV.01.005)

3.2. Normativos Externos:

a. Lei 13.709/18 – Lei Geral de Proteção de Dados (LGPD)
b. Marco Civil da Internet (Lei 12.965/2014)
c. Código de Defesa do Consumidor de 1990 (Lei 8.0787/1990 - Art.43)
d. ISO/IEC 27001 - Segurança da Informação

4. Definições

Com o objetivo de alinhar os conceitos e eliminar erros de interpretações, para fins dessa política apresentamos as seguintes denominações:

a) **Autoridade Nacional de Proteção de Dados (ANPD)**: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.
b) **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
c) **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
d) **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Cópia não controlada

e) **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;
f) **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;
g) **Encarregado de Proteção de Dados**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
h) **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
i) **Titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
j) **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;
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;

5. Princípios e Diretrizes

Os princípios e diretrizes sobre proteção de dados adotados pela CMOC Brasil visam garantir que todas as operações de tratamento realizadas internamente estejam em conformidade com as determinações da Lei 13.709/18 (LGPD).

A presente política estabelece boas práticas e diretrizes de governança para o tratamento de dados, conforme os seguintes princípios:

a. Princípio da Minimização
Garantir que o tratamento de dados pessoais seja realizado de forma minimizada, coletando apenas as informações estritamente necessárias para a finalidade pretendida. O tratamento deve observar os princípios da finalidade, necessidade e transparência, assegurando que os dados sejam utilizados de maneira clara e proporcional.

b. Privacidade no desenho (*Privacy by Design*)
A incorporação das diretrizes de proteção de dados deve ocorrer desde o desenvolvimento de projetos, aquisição de softwares ou qualquer novo tratamento de informações. A metodologia *Privacy by Design* deve ser aplicada, incluindo a avaliação de riscos por meio do Relatório de Impacto à Proteção de Dados Pessoais (INVDADDPIA), com suporte do Encarregado de Proteção de Dados. Esse relatório deve conter, no mínimo, a descrição dos dados coletados, finalidade do tratamento, metodologia empregada e as garantias de segurança adotadas para mitigar riscos.

c. Controles Internos e Gestão de Riscos
Identificar, documentar e comunicar ao Encarregado de Proteção de Dados quaisquer ameaças à segurança das informações. Cabe a esse profissional avaliar e, quando necessário, implementar medidas corretivas e controles adicionais para reduzir riscos financeiros, reputacionais e de conformidade.

d. Inventário de Dados e Descarte de Documentos
Manter atualizado o inventário de documentos físicos e eletrônicos que contenham dados pessoais, garantindo a rastreabilidade e correta destinação das informações. Após o cumprimento da finalidade para a qual os dados foram coletados, estes devem ser descartados, bloqueados ou anonimizados com segurança, conforme estabelecido na Política de Retenção e Descarte de Documentos Tratados.

e. Gestão de Contratos e Terceiros
Antes da contratação de fornecedores ou parceiros que realizem o tratamento de dados pessoais, deve ser realizada uma avaliação de conformidade com a LGPD. O processo de seleção deve considerar os controles de segurança adotados pelos terceiros e as medidas de mitigação de riscos e incidentes. A

Cópia não controlada

CMOC Brasil adota cláusulas específicas de adequação à LGPD em seus contratos, garantindo o cumprimento das obrigações legais.

f. Incidentes e Violações de Dados
Em caso de incidente envolvendo dados pessoais, a situação deve ser registrada, investigada e documentada, assegurando a comunicação tempestiva a todas as partes interessadas. O tratamento do incidente deve seguir os requisitos legais vigentes e as diretrizes do Plano de Ação, Comunicação e Resposta a Incidentes (PDD.01.003).

g. Segurança da Informação e Sistemas de TI
Os sistemas e processos que envolvem tratamento de dados pessoais devem ser desenvolvidos considerando os princípios do *Privacy by Design*. Devem ser aplicadas medidas técnicas adequadas para proteger os dados contra acessos não autorizados, destruição, perda, alteração ou divulgação indevida. O suporte e monitoramento dessas medidas serão conduzidos pelo Encarregado de Proteção de Dados, conforme estabelecido na Política de Segurança da Informação (STI.01.033) e na Política de Gestão de Identidade e Acessos (STI.01.063).

A CMOC realizará, no mínimo uma vez ao ano, revisão dos acessos de todos os colaboradores. O Encarregado de Dados, em conjunto com a equipe de TI e os gestores, avaliará os perfis e níveis de acesso, garantindo conformidade e prevenindo riscos. Situações de acesso incompatíveis ou que apresentem conflitos de interesse serão analisadas em detalhe para assegurar a integridade e privacidade das informações.

h. Melhoria Contínua
As políticas e procedimentos relacionados à Privacidade e Proteção de Dados da CMOC Brasil serão revisados a cada dois anos ou conforme orientação do Comitê de Governança de Dados (CGD), garantindo que reflitam as melhores práticas e sejam suficientes para mitigar os riscos emergentes.

A CMOC Brasil está comprometida com a garantia dos direitos dos titulares de dados, conforme os artigos 17 a 22 da LGPD, que incluem solicitações de confirmação, correção, portabilidade e exclusão de informações. Para tanto, disponibiliza canais de comunicação em suas plataformas para que os titulares possam exercer seus direitos de forma ágil e transparente.

6. Coleta, Armazenamento e Tratamento de Dados

Toda informação coletada, gerada, armazenada, processada, administrada ou confiada à CMOC Brasil é considerada propriedade da empresa e está regulamentada por esta Política de Privacidade e Proteção de Dados. Essas informações estão sujeitas a auditoria e monitoramento para garantir seu uso apenas por usuários devidamente autorizados e exclusivamente para fins profissionais.

Os gestores e colaboradores devem adotar todas as medidas estabelecidas nesta política ao tratar informações de clientes, fornecedores e colaboradores obtidas ou geradas durante suas atividades, especialmente no que se refere a dados pessoais e dados sensíveis.

Todos os colaboradores devem contribuir para a adoção de boas práticas e para o cumprimento dos seguintes objetivos:

a. Coleta e Consentimento
Garantir que a coleta de dados pessoais seja realizada de acordo com a necessidade e obrigatoriedade de obtenção de consentimento, conforme exigido pela LGPD. A coleta deve seguir as instruções recebidas pelos gestores, clientes, controladores ou outras entidades envolvidas. Sempre que necessário, deve-se garantir ao titular o acesso e a revisão das informações de forma gratuita e simplificada. O consentimento deve ser solicitado de maneira clara, permitindo que o titular escolha sobre o tratamento de seus dados, salvo exceções previstas na legislação vigente. Mudanças no tratamento de dados devem ser comunicadas com transparência, e um novo consentimento deve ser solicitado quando aplicável. O tratamento de dados pessoais de maneira discriminatória é expressamente proibido.

b. Tratamento de Dados

Cópia não controlada

Os dados de colaboradores, fornecedores e clientes, bem como aqueles gerados pelos colaboradores da CMOC Brasil, devem ser tratados exclusivamente para os fins a que se destinam. Todos os dados coletados, armazenados e processados devem ser classificados e protegidos adequadamente ao longo de seu ciclo de vida, considerando seu grau de confidencialidade e relevância.

c. Armazenamento
O armazenamento de dados deve ser realizado utilizando os recursos oficiais disponibilizados pela empresa, garantindo segurança e conformidade. Os dados pessoais devem ser mantidos apenas pelo tempo necessário para cumprir sua finalidade ou atender à legislação vigente, conforme estabelecido na Política de Retenção e Descarte de Documentos Tratados.

Caso o titular solicite a exclusão de seus dados, a CMOC acatará a menos que se enquadre nas seguintes situações:
- Cumprimento de obrigação legal;
- Necessidade de defesa em processos judiciais, administrativos ou arbitrais;
- Exercício regular de direitos contratuais ou legais;
- Proteção dos interesses da CMOC Brasil conforme os serviços contratados.

d. Compartilhamento de Dados
O compartilhamento de dados será permitido apenas mediante aprovação formal do titular, para cumprimento de obrigação legal ou quando necessário para atender à finalidade do tratamento, conforme as limitações da Lei 13.709/18 (LGPD). A CMOC Brasil não vende, compartilha ou comercializa dados pessoais coletados sem o consentimento prévio do titular.

e. Transferência Internacional de Dados
A transferência internacional de dados será realizada apenas quando forem garantidos os princípios e direitos do titular, conforme o artigo 33 da LGPD. Os titulares serão informados previamente sobre essa possibilidade e os mecanismos de proteção adotados.

f. Segurança da Informação
A CMOC Brasil adota medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados, bem como contra destruição, perda, alteração, comunicação ou difusão acidental ou ilícita.

g. Vazamento e Perda de Dados
A empresa deve aplicar todas as medidas disponíveis para garantir a segurança dos dados pessoais. Gestores e colaboradores têm a responsabilidade de informar imediatamente seus superiores ao identificar incidentes, violações, acessos indevidos ou perda de dados.

h. Prestacão de Contas
A CMOC Brasil deve adotar e demonstrar medidas de conformidade com a LGPD, assegurando que as diretrizes de proteção de dados sejam cumpridas e eficazes. Os titulares dos dados e órgãos de fiscalização devem ter acesso às informações sobre as práticas adotadas.

7. Direitos dos Titulares

A CMOC Brasil assegura aos titulares de dados pessoais o pleno exercício de seus direitos conforme previsto na Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018). Esses direitos incluem:

a) **Confirmação e Acesso aos Dados Pessoais:** O titular pode solicitar a confirmação da existência de tratamento de seus dados pessoais e obter acesso a esses dados de forma clara e completa, incluindo a finalidade e forma de processamento.
b) **Correção de Dados Incompletos, Inexatos ou Desatualizados**: Caso haja erros ou inconsistências nos dados tratados, o titular pode solicitar a retificação ou atualização das informações.
c) **Portabilidade dos Dados para Outro Fornecedor de Serviço:** O titular tem o direito de requisitar a transferência de seus dados a outra empresa ou organização, respeitando os regulamentos da Autoridade Nacional de Proteção de Dados (ANPD) e demais normas aplicáveis.
d) **Anonimização, Bloqueio ou Eliminação de Dados Desnecessários**: Quando os dados pessoais forem considerados excessivos ou não forem mais necessários para os fins específicos

Cópia não controlada

para os quais foram coletados, o titular pode exigir sua anonimização (de modo que não possam mais ser associados a uma pessoa), bloqueio ou exclusão.

e) **Revogação do Consentimento:** Nos casos em que o tratamento de dados for baseado no consentimento do titular, ele pode revogar sua autorização a qualquer momento, cessando o processamento dos dados, salvo quando houver outra base legal que justifique a continuidade do tratamento.

A CMOC Brasil se compromete a atender essas solicitações em conformidade com os prazos e procedimentos estabelecidos pela legislação vigente.

8. Tratamento de Dados Pessoais e Sensíveis

A CMOC Brasil realiza o tratamento de dados pessoais exclusivamente em conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) e de acordo com as instruções dos titulares. O tratamento ocorre nas seguintes hipóteses legais:
- Consentimento do titular, quando a CMOC Brasil atuar como controladora;
- Cumprimento de obrigação legal ou regulatória;
- Execução de contrato ou de procedimentos preliminares solicitados pelo titular;
- Atendimento a interesses legítimos, conforme previsto na LGPD.

O tratamento de dados pessoais sensíveis segue padrões rigorosos de segurança e só ocorre nas situações previstas no artigo 11 da LGPD, como consentimento explícito, cumprimento de obrigação legal, proteção da vida, tutela da saúde e prevenção à fraude.

A CMOC Brasil notificará imediatamente os titulares em caso de incidentes de segurança, como vazamento, perda ou acesso indevido de dados pessoais.

9. Tratamento de Dados Pessoais nas Mídias Digitais

A CMOC Brasil assegura a proteção dos dados pessoais coletados em seus canais digitais, adotando as seguintes diretrizes:
- Coleta de Dados: Os titulares serão informados previamente sobre a finalidade do tratamento de seus dados e, quando necessário, será solicitado consentimento explícito.
- Uso de Cookies: Cookies próprios e de terceiros são utilizados para personalizar conteúdos, fornecer funcionalidades e analisar tráfego, sempre mediante consentimento do titular.
- Compartilhamento com Terceiros: A CMOC Brasil pode compartilhar dados com operadores terceirizados, mediante contratos que garantem a privacidade e a proteção dos dados. No entanto, não se responsabiliza por sites e conteúdos externos e recomenda que os titulares consultem as políticas de privacidade dessas plataformas.

A CMOC Brasil não vende, compartilha ou comercializa dados pessoais coletados em suas mídias digitais.

10. Resposta a Incidentes e Violações

A CMOC Brasil adota um conjunto de ferramentas, controles preventivos e detectivos para monitorar e mitigar riscos relacionados ao tratamento de dados pessoais. O objetivo é prevenir incidentes que possam resultar em acessos indevidos, vazamento de informações, compartilhamento não autorizado, perda de dados e outras situações que possam comprometer a segurança da informação e a reputação da empresa, seus colaboradores, clientes e parceiros.

10.1. Medidas Preventivas e Monitoramento

Para fortalecer a segurança dos dados e minimizar o risco de incidentes, a CMOC Brasil implementa medidas como:
- Controles adicionais de login e senha para garantir a autenticação segura dos usuários;
- Monitoramento contínuo e rastreabilidade de acessos, permitindo a identificação de eventuais atividades suspeitas;

Cópia não controlada

- Revisão periódica de acessos e permissões, assegurando que apenas usuários autorizados tenham acesso às informações sensíveis;
- Protocolos de auditoria e conformidade, garantindo o alinhamento das práticas internas com as regulamentações de proteção de dados.

Essas ações permitem a detecção precoce de vulnerabilidades e a resposta rápida a qualquer evento que possa comprometer a segurança das informações tratadas pela empresa.

10.2. Plano de Ação e Resposta a Incidentes

Caso ocorra um incidente de segurança envolvendo dados pessoais, a CMOC Brasil agirá prontamente com base no Plano de Ação, Comunicação e Resposta a Incidentes (PDD.01.003), garantindo uma abordagem estruturada para contenção e mitigação de danos.

O processo de resposta inclui as seguintes etapas:

a) Identificação da gravidade e extensão do incidente, avaliando a possível repercussão sobre os titulares de dados e a empresa;
b) Identificação dos dados comprometidos e titulares afetados, assegurando a análise precisa do impacto;
c) Notificação e reporte ao Comitê de Governança de Dados, permitindo que a governança da empresa tome decisões estratégicas sobre o incidente;
d) Contenção do incidente, adotando medidas imediatas para minimizar seus efeitos e evitar agravamento;
e) Definição da estratégia de comunicação interna e externa, garantindo transparência e conformidade com os requisitos regulatórios;
f) Implementação de medidas corretivas e mitigatórias, visando reduzir danos e fortalecer as práticas de segurança da informação;
g) Elaboração e apresentação de relatórios detalhados sobre o incidente, identificando suas causas, impactos e ações tomadas para evitar recorrências;
h) Determinação de responsabilidades e definição de medidas de reparação, quando aplicável, para minimizar os danos aos titulares e à organização.

10.3. Comunicação e Transparência

A CMOC Brasil adotará as melhores práticas de comunicação para garantir que os incidentes sejam divulgados de forma clara e responsável, conforme sua gravidade e impacto. A divulgação poderá ser realizada por meio de:
- Canais internos e externos de comunicação, incluindo intranet, comunicados oficiais e site institucional;
- Notificações diretas aos titulares afetados, em conformidade com os requisitos estabelecidos pela LGPD e pela Autoridade Nacional de Proteção de Dados (ANPD);
- Relatórios de conformidade e segurança, compartilhados com os órgãos reguladores, quando necessário.

Além disso, a CMOC Brasil disponibiliza um canal direto para contato com o **Encarregado de Proteção de Dados (DPO)** para esclarecimento de dúvidas, solicitações e informações adicionais. O e-mail oficial para esse atendimento é: encarregadodados@br.cmoc.com.

Para garantir agilidade e imparcialidade no tratamento dos incidentes, as comunicações serão analisadas e processadas por um grupo multidisciplinar, minimizando riscos de conflito de interesses e assegurando a transparência e eficiência na resposta às ocorrências reportadas.

11. Papéis e Responsabilidades

A CMOC Brasil estabelece uma estrutura organizacional robusta para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), designando responsabilidades específicas para os diversos setores envolvidos na governança e proteção dos dados pessoais.

11.1. Comitê RiskCo

O Comitê RiskCo é responsável por supervisionar a governança e gestão de riscos relacionados à proteção de dados na CMOC Brasil. Suas atribuições incluem:

Cópia não controlada

a) Indicar o Encarregado de Proteção de Dados (DPO - *Data Protection Officer*), garantindo que a empresa tenha um profissional capacitado para atuar na gestão da privacidade;
b) Avaliar desvios de governança reportados pelo Comitê de Governança de Dados (CGD), utilizando o processo de classificação e reporte definidos na Matriz de Governança (GOVMATRIZ).

11.2. Encarregado de Proteção de Dados (DPO)

O Encarregado de Proteção de Dados (DPO) desempenha um papel fundamental na supervisão e implementação das práticas de privacidade e segurança de dados pessoais dentro da CMOC Brasil. Suas responsabilidades incluem:

a) Receber e responder a reclamações e comunicações dos titulares de dados, fornecendo esclarecimentos e adotando as providências necessárias;
b) Receber notificações da Autoridade Nacional de Proteção de Dados (ANPD) e tomar as medidas cabíveis para atender às exigências regulatórias;
c) Orientar empregados e contratados da CMOC Brasil sobre as diretrizes e melhores práticas de proteção de dados pessoais;
d) Implementar e supervisionar as políticas internas de privacidade e proteção de dados;
e) Organizar, presidir e oferecer suporte ao Comitê de Governança de Dados (CGD), auxiliando na tomada de decisões estratégicas sobre privacidade e segurança da informação;
f) Apoiar as equipes na adaptação de normas e procedimentos internos para garantir a conformidade com a LGPD;
g) Identificar e avaliar riscos e ameaças à segurança dos dados pessoais tratados pela empresa;
h) Propor medidas de mitigação de riscos e, caso sejam aprovadas, garantir sua implementação e monitoramento;
i) Supervisionar incidentes de segurança e garantir a comunicação eficiente de violações de dados à ANPD e aos titulares afetados, dentro de prazos razoáveis, sempre que houver risco ou dano relevante.

§ parágrafo único: A CMOC Brasil estabeleceu internamente que a comunicação oficial com a ANPD será conduzida exclusivamente pelo **Gerente de Relações Governamentais**.

11.3. Comitê de Governança de Dados (CGD)

O Comitê de Governança de Dados (CGD) é nomeado por esta política e é composto por representantes das seguintes áreas da CMOC Brasil:
- Relações Governamentais,
- Gestão de Contratadas,
- Tecnologia da Informação,
- Jurídico,
- Governança,
- Recursos Humanos (RH),
- Encarregado de Proteção de Dados (DPO), que será responsável pela coordenação do comitê.

As principais responsabilidades do CGD são:

a) Revisar e aprovar a Política de Proteção de Dados da CMOC Brasil, garantindo sua conformidade com as diretrizes regulatórias;
b) Analisar relatórios de impacto à proteção de dados e sugerir melhorias para a gestão da privacidade;
c) Avaliar incidentes de segurança de dados pessoais, analisando suas causas, impactos e ações corretivas necessárias;
d) Definir e supervisionar a estratégia de comunicação de incidentes junto à diretoria e à área de comunicação institucional;
e) Aprovar medidas de mitigação de riscos e novos procedimentos voltados à proteção de dados pessoais;
f) Avaliar a eficácia das medidas adotadas para contenção e reparação de danos em casos de violações de dados;
g) Opinar sobre a forma e alcance das eventuais reparações de danos aos titulares afetados;
h) Assegurar que a organização disponha de recursos adequados para uma gestão eficaz da proteção de dados pessoais;
i) Promover a disseminação da cultura de proteção de dados por meio da comunicação e treinamento contínuos, garantindo que as políticas e procedimentos sejam amplamente divulgados e compreendidos.

Cópia não controlada

11.4. Tecnologia da Informação (TI)

A equipe de Tecnologia da Informação (TI) desempenha um papel crucial na implementação e manutenção das medidas de segurança de dados. Suas principais responsabilidades incluem:

a) Incorporar os requisitos estabelecidos nesta política nos procedimentos e diretrizes do departamento de TI;
b) Implementar controles de segurança eficazes para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação indevida ou qualquer outro tipo de tratamento inadequado, conforme as diretrizes mínimas recomendadas pela ANPD;
c) Apoiar o Encarregado de Proteção de Dados (DPO) e os titulares de dados na resposta a incidentes de segurança, garantindo a rápida contenção e mitigação de riscos sempre que houver impacto relevante.

11.5. Usuários

Todos os colaboradores, parceiros e prestadores de serviços da CMOC Brasil são responsáveis por cumprir integralmente as diretrizes estabelecidas nesta Política de Proteção de Dados. Suas obrigações incluem:

a) Ler, compreender e seguir sem exceções as diretrizes previstas na Política de Proteção de Dados da empresa;
b) Reportar ao Encarregado de Proteção de Dados (DPO) qualquer risco ou vulnerabilidade identificada que possa comprometer a segurança das informações;
c) Comunicar imediatamente ao DPO qualquer evento ou incidente que possa violar a política de proteção de dados ou representar risco aos titulares;
d) Assinar e cumprir os Termos de Responsabilidade e quaisquer outros documentos que formalizem o compromisso com as boas práticas de privacidade e proteção de dados.

12. Sanções

O descumprimento das diretrizes estabelecidas nesta Política de Proteção de Dados e nos procedimentos internos relacionados à privacidade e segurança da informação poderá resultar na aplicação de penalidades proporcionais à gravidade da infração, conforme descrito abaixo.

12.1. Sanções para Colaboradores da CMOC Brasil

Os colaboradores da CMOC Brasil que cometerem violações, desvios de conduta ou negligências em relação a esta política, seja por ação direta, omissão, tentativa de descumprimento ou falha involuntária, estarão sujeitos a penalidades que incluem:
- Advertência verbal, para infrações leves ou eventuais falhas de conformidade;
- Advertência por escrito, em casos de reincidência ou descumprimento de diretrizes críticas;
- Suspensão não remunerada, quando houver impacto significativo para a organização ou riscos à proteção de dados;
- Demissão por justa causa, para infrações graves que comprometam a privacidade dos titulares de dados, causem danos à empresa ou violem princípios fundamentais da Lei Geral de Proteção de Dados (LGPD).

As penalidades serão aplicadas conforme a gravidade da infração e as disposições previstas no contrato de trabalho da CMOC Brasil.

12.2. Sanções para Colaboradores de Terceiros Contratados

No caso de terceiros contratados que tenham acesso a dados pessoais e violem esta política ou qualquer outro procedimento interno relacionado à proteção de dados, as penalidades poderão incluir:
- Notificações formais por escrito, registrando o descumprimento e exigindo adequação às diretrizes da empresa;
- Retratações institucionais, caso o incidente comprometa a reputação ou a imagem da CMOC Brasil;
- Reparação financeira, em casos em que o descumprimento gere prejuízos financeiros ou legais à organização;

Cópia não controlada

- Término do contrato de prestação de serviços, nos casos mais graves ou quando houver reincidência de falhas que comprometam a segurança da informação e a proteção de dados pessoais;
- Aplicação de outras sanções previstas nos contratos firmados com a CMOC Brasil.

12.3. Responsabilidade de Terceiros no Tratamento de Dados

Empresas contratadas que realizam o tratamento de dados pessoais em nome da CMOC Brasil assumem a corresponsabilidade pelo cumprimento das diretrizes estabelecidas nesta política e na legislação aplicável.

Caso descumpram essas diretrizes, estarão sujeitas a sanções administrativas, contratuais ou até mesmo ao encerramento do contrato, além das penalidades previstas na LGPD e em outros regulamentos pertinentes.

A CMOC Brasil reforça seu compromisso com a proteção de dados pessoais e espera que todos os colaboradores, fornecedores e parceiros sigam rigorosamente as diretrizes estabelecidas, garantindo a conformidade com a legislação vigente e a segurança da informação em todas as operações da empresa.

13. Confidencialidade dessa Política

Este documento é de propriedade da CMOC Brasil, porém, em virtude de suas características, sua consulta é permitida. É vedada a sua reprodução, distribuição ou modificação sem autorização expressa do Comitê de Governança de Dados.

Cópia não controlada