Relatório de Impacto à Proteção de Dados Pessoais

Março de 2024

Sumário

1 Identificação dos Agentes de Tratamento e do Encarregado

	Controlador: Oliveira Filtros	Operador: Não se aplica
	Encarregado: Jackson Alex Vinotti - Advogado (OAB/SC 56.492 | OAB/PR 92.992)	
	E-mail Encarregados: dpo.oliveirafiltros@gmail.com	Telefone Encarregados: (47) 3642-1609

2 Necessidade de Elaborar o Relatório

A Política de Conformidade (*Compliance*) da Oliveira Filtros (PCO-OF) tem entre seus objetivos assegurar que as atividades da Oliveira Filtros sejam conduzidas em conformidade com as normas aplicáveis à Empresa, sob a coordenação do Escritório Rocha & Vinotti Advocacia, sob os titulares Dr. Jackson Alex Vinotti (OAB/SC 56.492 | OAB/PR 92.992) e Dr. Philipe Gustavo Portela Pires (OAB/SC 64.739).

Nesse sentido, de acordo com o art. 38, *caput*, da Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), a qualquer momento a Autoridade de Proteção de Dados Pessoais (ANPD) pode determinar ao Oliveira Filtros que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis. Surgiu, assim, a necessidade de se confeccionar este documento.

A Oliveira Filtros realiza diariamente o tratamento[1] dos dados pessoais que se relacionam com a pessoa natural identificada ou identificável (art. 5º, I, da LGPD). Existem também os dados pessoais sensíveis, que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (art. 5º, II, da LGPD).

[1] 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 (art. 5º, X, da LGPD).

Considerando os fundamentos[2] da proteção de dados pessoais (art. 2º da LGPD), a boa-fé e os demais princípios[3] a serem observados nas atividades de tratamento de dados pessoais (art. 6º da LGPD), a Oliveira Filtros dispõe de diferentes sistemas de controles internos, que variam de acordo com a natureza do dado pessoal, para mitigar eventuais riscos de falha na proteção de dados pessoais.

Entretanto, apesar do elevado grau de maturidade da gestão de riscos da Oliveira Filtros, não se pode garantir a eliminação total dos riscos que, em caso de materialização, causariam impacto à privacidade dos dados pessoais existentes na empresa.

3 Descrição do Tratamento

A Política de Segurança e Privacidade da Oliveira Filtros, visa orientar as ações necessárias à garantia da segurança da informação, o que resulta na mitigação de riscos aos quais estão sujeitos os ativos de informação e que poderiam comprometer as atividades da Oliveira Filtros e o cumprimento de sua missão institucional.

[2] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

[3] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII – segurança: utilização de medidas 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 difusão; VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

No que se refere especificamente às informações de caráter pessoal, os sistemas de controle interno implantados na Oliveira Filtros variam de acordo com o tipo de suporte (físico ou digital), bem como com a natureza da informação (comum ou sensível).

Nesta seção, são descritos os processos de tratamento de dados pessoais, digitais ou físicos, que podem gerar riscos às liberdades civis e aos direitos fundamentais, envolvendo a especificação de natureza,[4] escopo,[5] contexto[6] e finalidade[7] do tratamento.

3.1 Descrição do tratamento

3.1.1 Natureza do tratamento

São adotadas medidas 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 difusão.

O acesso às bases de dados é controlado por grupos de rede e acesso limitado a determinados perfis de usuários. Há contínua busca por segurança da informação ao se fazer uso de sistemas corporativos na Oliveira Filtros e ao dar cumprimento às disposições contidas na Política de Segurança e Privacidade.

Como medidas administrativas adotadas, citam-se: i) Adoção da Política de Privacidade clara e transparente; ii) Informação do tratamento dos dados pessoais a clientes; iii) assinatura de acordos de responsabilidade para acesso a sistemas, por requisição formal ou por *e-mail*; vi) registro dos acessos concedidos; e v) destacamento de funcionários dedicados às respostas das demandas de outros poderes, com criação de diretórios de acesso exclusivo para guarda de documentos digitais

3.1.2 Natureza do tratamento

[4] A natureza representa como a instituição pretende tratar ou tratar os dados pessoais.
[5] O escopo diz respeito à abrangência do tratamento de dados.
[6] O contexto destaca um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.
[7] A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais, justifica o tratamento e fornece os elementos para informar o titular dos dados.

Existem diversas formas de tratamento dos dados pessoais na Oliveira Filtros, considerando a definição da LGPD:

- Coletados/Enviados

Os dados são coletados principalmente por meio dos dados fornecidos pelos clientes que adquirem os produtos e serviços oferecidos pela Olivera Filtros, e por aquisições de dados através de incorporações de empresas, em que ocorreram a recepção e processamento de dados pessoais identificados pelo tipo e finalidade identificados neste RIPD. Tanto as novas captações de informação quanto às novas bases de dados criadas são objeto de análise no âmbito da governança da informação, observando a devida adequação à LGPD.

A Oliveira Filtros, por meio de seus serviços digitais, pode ainda captar informações fornecidas por pessoas físicas, usuárias desses serviços. A captação e o uso desses dados se sujeitam à Política de Privacidade e Termos de Uso do *site*, dos serviços digitais e da venda de produtos em suas lojas.

- Retidos/Armazenados

Os dados são mantidos em sistemas gerenciadores de banco de dados e em servidores de arquivos, nos quais os acessos são restritos, de acordo com os conteúdos armazenados.

- Usados

Os dados são usados em processos de trabalho das unidades da Oliveira Filtros (também chamadas neste relatório de Departamentos), em agregações analíticas ou em análises singulares, quando pertinente ao processo de trabalho do departamento e com justificada finalidade.

- Eliminados

O curador[8] pode indicar no Catálogo de Informações[9] que uma base de dados deve ser desativada. Nesse caso, deve-se optar por arquivamento (com a criação de um backup e manutenção de curadoria) ou por descarte, quando os dados são apagados, e deve ser fornecida uma justificativa para a desativação.

O Controlador executa processo para a desativação de bases de dados, que inclui avaliação do uso dos dados na Oliveira Filtros. Inicialmente, retiram-se os acessos de escrita, em seguida os de leitura, e, por fim, são eliminadas todas as conexões, para posterior exclusão dos dados. Esse procedimento permite a descoberta de eventuais usuários dos dados antes da eliminação.

3.1.3 Fonte dos dados

As formas de coleta de dados na Oliveira Filtros são:

- captações de informações externas: são enviados arquivos de dados com informações pessoais incorporadas e sujeitas ao tratamento de dados e as Políticas de Segurança e Privacidade da Oliveira Filtros (PSPOF);
- sistemas de informação: site;
- recebimento de documentos e formulários: eletronicamente ou em papel; e,
- registro de informações pelos atendimentos institucionais: presencial e telefônico.

3.1.4 Compartilhamento de dados

A Oliveira Filtros compartilha dados com seus colaboradores, provedores de serviços parceiros que atuam em nosso nome, serviços de TI e com empresas afiliadas e parceiras de negócios a serviços da Oliveira Filtros com autorização expressa ou presumida do titular. A Oliveira Filtros também pode compartilhar os dados com órgãos dos Poderes Judiciário, Executivo e Legislativo, e do Ministério Público, para fins de instrução de processo de apuração de

[8] Responsável pela base de dados departamental.

[9] Catálogo de metadados sobre as bases de dados divulgadas, para permitir o entendimento necessário à utilização dos dados, abrangendo também a indicação dos responsáveis pela sustentação de cada base de dados divulgada, de acordo com a Política de Segurança e Privacidade da Oliveira Filtros.

irregularidades em que o titular das informações estiver envolvido, bem como com autorização judicial.

No Catálogo de Informações da Oliveira Filtros, o curador pode definir os canais de publicação externa de cada base de dados. São informações sobre a base de dados como um todo, mas o curador pode informar se existem dados pessoais.

3.1.5 Adoção de nova tecnologia para tratamento de dados

A adoção de novas tecnologias para tratamento dos dados é objeto de permanente atenção da Oliveira Filtros, no sentido de garantir a conformidade com a LGPD, em particular os direitos dos titulares dos dados pessoais.

3.1.6 Medidas de segurança

A segurança da informação é constantemente revista e aprimorada com novas medidas de segurança. Uma das abordagens em discussão atualmente é garantir que os dados estejam protegidos durante todo o seu tratamento (desde a coleta até a eliminação). Nesse processo, são utilizados diversos sistemas, tecnologias e ferramentas para permitir a criptografia e o controle de acesso de forma integrada.

A Política de Segurança e Privacidade da Olveira Filtros (PSPOF) é regida pelos seguintes princípios da segurança da informação: disponibilidade; integridade; confidencialidade; autenticidade; irretratabilidade; privilégio mínimo; necessidade de conhecer; proteção dos dados pessoais; e proteção da privacidade.

Esses princípios e as diretrizes constantes na PSPOF visam à garantia da segurança da informação da Oliveira Filtros, independentemente do meio em que ela se encontre.

Ressalta-se que os ativos de informação destinados à eliminação, seja em meio físico ou digital, são devidamente inutilizados, assegurando a segurança da informação e o atendimento aos princípios que regem a PSPOF.

3.1.7 Fluxo de dados

Os dados coletados e, eventualmente, compartilhados pela Oliveira Filtros trafegam pelos sistemas PDV, RHS e ERP, por rede privada, sendo que a base de dados possui um servidor próprio. A empresa MHS construiu o servidor da Oliveira Filtros com toda lógica de segurança e proteção das informações, a estrutura usa IP fixo[10] e tem armazenamento seguro dentro da estrutura do controlador que é o único a possuir acesso.

PDV: O sistema de ponto de venda (PDV), desenvolvido pela CH Sistemas e mantido pela MHS, representante de São Bento do Sul, engloba funcionalidades como gestão de caixa, emissão de cupons fiscais, e aceitação de pagamentos tanto de Pessoa Física quanto jurídica, incluindo transações por cartão de crédito. Sistema próprio desenvolvido pela RHS, trata-se de um programa interno da empresa e desenvolvido exclusivamente para o Oliveira Filtros, que possui todo o código fonte e banco de dados, sendo este usado somente com rede interna, sem acesso externo, somente para carteira de cliente, sem conexão com sistema de vendas.

MHS[11]: O módulo de recursos gera relatórios abrangendo informações detalhadas dos clientes, tais como nome, contato, data da última compra, próxima data de vencimento, endereço, referência, CPF/CNPJ, além do contato do responsável pela residência ou empresa, detalhes dos produtos adquiridos e observações relevantes, tanto financeiras quanto relacionadas à localização. É importante ressaltar que as referências incluem dados sensíveis, como apelidos, características físicas e informações de confirmação estética do responsável.

ERP[12]: O sistema de planejamento de recursos empresariais, desenvolvido pela CH Sistemas e mantido pela MHS, com representação em São Bento do Sul, abrange um módulo de ordem de serviço (OS) que é pago mensalmente e está integrado ao órgão fiscal, permitindo acesso ao banco de dados do Governo Federal e à Receita Federal. Cada funcionário da empresa possui acesso

[10] Um endereço IP fixo, também conhecido como endereço IP estático, é um endereço único atribuído a um dispositivo em uma rede que permanece constante ao longo do tempo. Ao contrário de um endereço IP dinâmico, que pode mudar sempre que o dispositivo se reconecta à rede, um endereço IP fixo é estático e não muda, proporcionando consistência e previsibilidade na identificação e comunicação com o dispositivo dentro da rede ou na internet. Os endereços IP fixos são frequentemente utilizados em ambientes onde é necessário acesso remoto consistente a dispositivos, como servidores, câmeras de segurança ou dispositivos de rede, facilitando sua localização e gerenciamento.

[11] Sistema desenvolvido pela RHS - https://rhsinfo.com.br/

[12] Sistema desenvolvido pela RHS - https://rhsinfo.com.br/

limitado às funcionalidades do sistema, que gera relatórios detalhados de vendas, produtos, serviços e movimentações de ordem de serviço e nota fiscal.

Os sistemas permitem *download* de dados. Estes, por medida de segurança, são criptografados, mas podem ser descriptografados por uso de *software* específico.

Tanto o MHS quanto o ERP possuem acesso remoto pela desenvolvedora RHS, com segurança qualificada e registrada para prestação de serviço de manutenção, atualização e correção de possíveis erros de sistema, não tendo o acesso ao banco de dados.

Os usuários de serviços digitais fornecidos pela Oliveira Filtros podem, ainda, informar seus dados pessoais, conforme cada serviço e de acordo com os seus termos de uso.

Dentro do fluxo de dados o tratamento de informações obrigatórias relacionadas às vendas e prestações de serviço geram notas fiscais conforme a Lei 8.846/1994, a qual tem tratamento de compartilhamento de dados com o serviço de contabilidade prestado pelo contador Júlio Cesar Kujavski - Rua Nicolau Bley Neto, 100, S 5 CEP: 89300-000 – Mafra/SC.

São os dados tratados em compartilhamento com o profissional:

1. Informações do Emitente e do Destinatário: Nome ou razão social, endereço completo, CPF ou CNPJ (Cadastro Nacional da Pessoa Jurídica), inscrição estadual, e outras informações de identificação tanto do emissor quanto do destinatário da nota fiscal.
2. Detalhes da Transação: Descrição dos produtos ou serviços vendidos, quantidade, preço unitário, valor total da transação, impostos aplicáveis, descontos concedidos, e quaisquer outras condições comerciais relevantes.
3. Informações Fiscais: Número da nota fiscal, data de emissão, data de saída ou prestação do serviço, código fiscal de operações e prestações (CFOP), regime tributário aplicável, e outras informações fiscais exigidas pelas autoridades competentes.
4. Identificação da Operação: Indicação se a operação é de venda, prestação de serviço, transferência, devolução, entre outros tipos de transações comerciais.
5. Dados de Controle e Rastreamento: Números de série ou lotes dos produtos, informações de transporte e entrega, forma de pagamento, dados bancários, e

quaisquer outras informações necessárias para controle e rastreamento da operação.

Todas as notas de serviços são emitidas pela empresa de Mafra/SC, já as de produtos são de acordo com a venda podendo ser emitida por Mafra/SC ou na filial em Rio Negro/PR.

Os fluxos em cada uma das operações são:

Serviços (PDV/MHS/ERP): Cadastro pelo setor comercial e venda > elaboração da Ordem de Serviço (OS) > envio para o operador > prestação de serviço > retorno de comunicação ao setor comercial e financeiro > atualização de cadastro com as informações coletadas do serviço e/ou equipamentos > Contador > emissão de NFe > baixa do serviço > atualização de cadastro para novos agendamentos e produção de relatório de pagamento.

Produtos (PDV/MHS/ERP): Cadastro pelo setor comercial > separação e/ou aquisição de produto e peças > envio para o operador > entrega ou retirada em loja > retorno de comunicação ao setor comercial e financeiro > atualização de cadastro com as informações coletadas do serviço e/ou equipamentos com reserva de dados para garantia dos produtos e equipamentos.

Para o tratamento de dados financeiros em vendas de Cartão de Crédito os sistemas bancários utilizados são com o banco Sicoob (SIPAG) e Stone (TON) que somente tem acesso pelos operadores através de registros nos próprios sistemas bancários que são qualificados e arquivados nos próprios operadores externos e junto ao BACEN que efetiva o registro de vendas feitas à crédito no Brasil.

Somente o financeiro tem acesso sistema de relatórios através de aplicação própria do sistema de gestão dos bancos. O setor financeiro ainda detém, sobre registro automatizado em nome de cada operador o acesso à: vendas, financeiro, caixa, notas de produtos comprados e vendidos, devedores, formas de pagamento e aos sistemas ERP, PDV e RHS.

Observa-se que todo o tratamento de dados ocorre de forma integrada entre empresas, mesmo que se efetive algum serviço ou venda para pessoa física, todos os registros são B2B.

3.2 Dados físicos

A Oliveira Filtros possui e trata dados físicos, são eles os relatórios mensais de clientes e serviços, relatório financeiro de pagamentos, compras, vendas, serviços com prazo e inadimplentes,

recibos de comprovantes de pagamentos e recibos de venda de cartão de crédito, certificados de venda e de garantias dos produtos. Os dados são tratados tanto na matriz em Mafra/SC como na filial em Rio Negro/PR.

Todos os documentos físicos estão guardados, armazenados e arquivados nas estruturas da empresa de forma segura, com acesso exclusivo da controladora e bem como sob acesso a cada operador por setor e somente quando necessário, sendo registrado o uso de cada documento.

A cultura de sustentabilidade da empresa faz uso de papéis para rascunho, contudo todas as informações de dados e identificação são rasuradas para que não possam ser identificadas. Além disso, todos os papéis são **eliminados de forma conjunta e mensalmente,** através de incineração para eliminação de todos os dados.

3.3 Escopo do tratamento

O escopo representa a abrangência do tratamento de dados.

Conforme visto na seção 3.2 deste Relatório, os dados contidos em documentos físicos recebem o mesmo tratamento dos digitais, pois são digitalizados assim que adentram no Protocolo da Oliveira Filtros.

Os dados digitais coletados estão previstos no PSPOF, bem como sua finalidade e prazo de armazenamento, cujas bases de dados são divulgadas no site da Oliveira Filtros.

As seções seguintes mostram detalhes sobre a extensão do escopo para os dados digitais.

3.3.1 Tipos de dados

O inventário das bases de dados da Oliveira Filtros está disponível em: https://www.casadosfiltrosmafra.com/.

3.3.2 Frequência de tratamento dos dados

A Oliveira Filtros trata dados pessoais diariamente, por seus sistemas de informação, conforme estabelecido pelas finalidades e pelos regulamentos de cada sistema.

3.3.3 Retenção dos dados

No PSPOF, o curador pode definir o tempo de retenção e de descarte para cada base de dados, observando a finalidade, a legislação e os normativos vigentes. Essas informações dizem respeito a toda a base de dados, e não especificamente aos dados pessoais nela contidos.

3.3.4 Titulares afetados pelo tratamento de dados

Qualquer pessoa física ou jurídica, cliente ou usuária de serviços e produtos fornecidos pela Oliveira Filtros, pode ser afetada pelo tratamento de dados na Oliveira Filtros.

3.4 Finalidade do tratamento

O tratamento de dados pessoais é uma atividade essencial para a prestação de serviços e venda dos produtos comercializados pela Oliveira Filtros. Na Olivera Filtros, os dados são usados principalmente para:

- promover a entrega e/ou prestação de dos serviços contratados;
- enviar anúncios e ofertas, newsletter/e-mail marketing e comunicação da validade dos produtos;
- análise e proteção ao crédito;
- responder solicitação dos usuários;
- análise de processo seletivo ou admissional; e,
- aprimoramento estratégico dos usuários dentro das plataformas digitais.

4 Partes Interessadas Consultadas

Para a elaboração deste Relatório, todas as unidades da Oliveira Filtros foram consultadas. As avaliações de conformidade à LGPD iniciaram em novembro de 2023 a março de 2014, segundo

padrão metodológico desenvolvido pelo Rocha & Vinotti Advocacia, baseado nas melhores práticas de gerenciamento de conformidade.

5 Necessidade e Proporcionalidade

O tratamento de dados é limitado ao mínimo necessário para a realização das finalidades informadas ao titular. Quando necessário, tem abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

O tratamento é feito apenas quando é indispensável e com o propósito de promover o regular funcionamento das operações de venda promovidas pela empresa.

Com o objetivo de assegurar que o operador realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela empresa, todo colaborador ou terceirizado deve seguir as diretrizes previstas nas Políticas e demais documentos regulatórios dos tratamentos de dados.

Além disso, os sistemas de informação possuem logs e controles de acesso.

6 Riscos à Proteção de Dados Pessoais

A Oliveira Filtros identifica e avalia os riscos e impactos associados ao tratamento de dados pessoais, dos quais destacam-se os riscos à proteção de dados e informações armazenadas pela empresa, em especial aos dados pessoais.

6.1 Identificação de riscos

Neste campo avaliado considera-se válida a atuação da empresa dos referidos dados preservando a privacidade conforme preceitua o Art. 1º; Art. 2º, I; Art. 17; Art. 50, I, d) e II. Para tal, os principais pontos de tratamentos que permeiam a privacidade são:

Contato virtual e presencial com clientes:	para enviar produtos e orçamentos, agendar visitas, prestar suporte técnico e realizar cobranças;

Gestão de vendas e financeira:	para analisar o perfil dos clientes, segmentar ofertas, realizar cobranças, enviar documentos para pagamento e realizar campanhas de marketing;
Cumprimento de obrigações legais:	para emitir notas fiscais, contratos e outros documentos.

A natureza dos dados que a Oliveira Filtros coleta considerados sensíveis, como dados bancários e informações sobre saúde (em casos de filtros para purificação de água potável). Estes dados exigem um cuidado especial no tratamento, pois podem ser utilizados para fins discriminatórios ou fraudulentos. Por isso deve-se sempre, quando necessário serem tratados ter o registro dos tratamentos feito pelo operador que tiver acesso aos dados.

A coleta de dados é realizada por diversos canais, como website, telefone, e-mail, apps e presencialmente, o que dificulta o controle sobre o acesso e uso dos dados. Por isso os cadastros e usos devem sempre passar por registros dos operadores através dos sistemas e também de arquivos de ordem de serviço (OS).

Em virtude da introdução da temática de proteção dos dados pessoais, a metodologia de gestão de riscos operacionais da Oliveira Filtros passou por recente inclusão de novas taxonomias para identificação e mensuração dos riscos específicos a esse assunto. No levantamento dos riscos operacionais à proteção de dados pessoais, os eventos potenciais são analisados nas seguintes categorias:

1. Acesso não autorizado	Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.
2. Modificação não autorizada	Modificação de dados pessoais sem a anuência do titular; viola o princípio da segurança.
3. Perda	Destruição ou extravio de dados pessoais; viola os princípios da segurança e da prevenção.
4. Apropriação	Apropriação ou uso indébito de dados de pessoais; possibilidades de fraude e vazamento intencional de dados; viola os princípios da segurança e da prevenção.
5. Remoção não autorizada	Retirada de dados pessoais sem autorização do titular.
6. Coleção excessiva	Extração de mais dados do que o necessário para a realização do trabalho, ou do que é previsto em Lei ou foi autorizado pelo

	usuário; viola o princípio da necessidade.
7. Informação insuficiente sobre a finalidade do tratamento	A finalidade declarada para o uso das informações pessoais é insatisfatória, não é específica ou pode suscitar interpretações diversas.
8. Tratamento sem consentimento do titular dos dados pessoais	Tratamento dos dados pessoais sem a devida prévia permissão expressa, inequívoca e informada do titular, salvo exceções legais.
9. Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Compartilhamento dos dados pessoais com outras entidades privadas (fora da administração pública federal) sem a devida permissão do titular
10. Retenção prolongada de dados pessoais sem necessidade	Manter os dados pessoais do titular para além do necessário ou do que estava consentido/autorizado; viola o princípio da necessidade
11. Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	Erro ao vincular dados do verdadeiro titular a outro; viola o princípio da qualidade dos dados.
12. Falha ou erro de processamento	Processamento dos dados de forma imperfeita ou equivocada. Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc. Viola o princípio da qualidade dos dados.
13. Reidentificação de dados pseudonimizados	Anonimização insatisfatória de dados pessoais sensíveis possibilitando inferir quem é a pessoa em questão; viola o direito à anonimização.

6.2 Medidas de tratamento dos riscos

A aplicação da metodologia de identificação e avaliação dos riscos permite classificá-los de acordo com critérios de priorização. Assim, após a validação do tratamento pela alta administração, as ações necessárias para mitigar os riscos são formalizadas.

Dessa forma, passamos para uma análise minuciosa em que: P = Probabilidade e I = Impacto. Aplicam-se as definições de Probabilidade e Impacto para verificação do Nível de Risco Residual (NRR) em conformidade com a LGPD e a ISO 27701.

A ISO 27701 é uma extensão da norma ISO/IEC 27001, voltada para sistemas de gestão de segurança da informação (SGSI), que aborda especificamente a privacidade da informação.

Publicada em 2019, a ISO 27701 proporciona diretrizes para estabelecer, implementar, manter e aprimorar um sistema de gestão de privacidade da informação (SGPI).

A tabela a seguir apresenta o efeito resultante do tratamento do risco com a aplicação das medidas descritas na tabela. As seguintes opções podem ser utilizadas: Reduzir, Evitar, Compartilhar e Aceitar.

Risco	Medida(s)	Efeito sobre o Risco	Risco Residual		
			P	I	Nível (P x I)
R01 - Acesso não autorizado	1. Controle de acesso lógico[I] 2. Controles de segurança em redes/sistemas[II] 3. Proteção física do ambiente[III] 4. Auditoria[VIII]	Reduzir	5	15	75
R02 - Coleção excessiva	1. Limitação de coleta[VII] 2. Auditoria[VIII]	Reduzir	5	5	25
R03 - Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	1. Controle de acesso lógico[I] 2. Controles de segurança em redes/sistemas[II] 3. Proteção física do ambiente[III] 4. Limitação da coleta[VII] 5. Auditoria[VIII]	Reduzir	5	10	50
R04 - Falha em considerar os direitos do titular dos dados pessoais (ex: perda do direito de acesso)	1. Auditoria[VIII]	Reduzir	5	5	25
R05 - Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.)	1. Controle de acesso lógico[I] 2. Controles de segurança em redes/sistemas[II] 3. Proteção física do ambiente[III] 4. Continuidade de negócio[IV] 5. Cópia de segurança[V]	Reduzir	5	15	75
R06 - Informação insuficiente sobre a finalidade do tratamento	1. Auditoria[VIII]	Reduzir	5	5	25
R07 - Modificação não autorizada	1. Controle de acesso lógico[I] 2. Controles de segurança em redes/sistemas[II] 3. Proteção física do ambiente[III] 4. Continuidade de negócio[IV] 5. Cópia de segurança[V]	Reduzir	5	5	25

R08 - Perda	1. Controle de acesso lógico[I] 2. Controles de segurança em redes/sistemas[II] 3. Proteção física do ambiente[III] 4. Continuidade de negócio[IV] 5. Cópia de segurança[V]	Reduzir	5	5	25
R09 - Reidentificação de dados pseudonimizados	1. Controles criptográficos[VI]	Reduzir	5	5	25
R10 - Remoção não autorizada	1. Controle de acesso lógico[I] 2. Controles de segurança em redes/sistemas[II] 3. Proteção física do ambiente[III] 4. Continuidade de negócio[IV] 5. Cópia de segurança[V]	Reduzir	5	5	25
R11 - Retenção prolongada de dados pessoais sem necessidade	1. Auditoria[VIII]	Reduzir	5	5	25
R12 - Roubo	1. Controle de acesso lógico[I] 2. Controles de segurança em redes/sistemas[II] 3. Proteção física do ambiente[III] 4. Continuidade de negócio[IV] 5. Cópia de segurança[V]	Reduzir	5	15	75
R13 - Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente)	1. Auditoria[VIII]	Reduzir	5	10	50
R14 - Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular	1. Auditoria[VIII]	Reduzir	5	10	50

Planilha 1 - Impacto de não conformidade e urgência para ação

As normas brasileiras e a ISO 27701, que é internacional, enfatizam a importância da proteção da privacidade no contexto da segurança da informação e destaca a necessidade de integrar práticas de privacidade eficazes aos SGSI já existentes.

Assim, ao analisar a Planilha 1, verifica-se que todas as avaliações foram aferidas com grau de urgência para ação média ou baixa, ou seja, na percepção das unidades, os controles implantados são considerados adequados para garantir o razoável cumprimento da LGPD.

6.3 Criticidade

A partir da composição do impacto da não conformidade e da urgência para ação, encontra-se o grau de criticidade da obrigação avaliada. Atualmente todas as avaliações possuem criticidade baixa, fruto da implantação de ações de conformidade.[13]

6.4 Possíveis causas de não conformidade

Outro fator importante para auxiliar o planejamento de ações de conformidade pelas unidades é a identificação de possíveis causas de não conformidade. Na Planilha 1, pode ser vista a distribuição das causas apontadas nas avaliações, que atualmente, em sua totalidade, são não críticas.[14]

6.5 Ações de conformidade

Como resultado das avaliações realizadas, a Oliveira Filtros se compromete a implementar as seguintes ações de conformidade:

I. Adotar uma Política de Privacidade clara e transparente: a política deve informar aos clientes quais dados pessoais são coletados, como são utilizados e quais são os seus direitos;

[13] Ação definida para prevenção, identificação e correção de procedimentos que facilitem a ocorrência de falhas de conformidade, como por exemplo, implantação ou melhoria de controles e alterações normativas.
[14] Consideram-se não críticas as avaliações aferidas com graus de criticidade médio e baixo.

II. Obter o consentimento livre e informado dos clientes para o tratamento de seus dados pessoais: o consentimento deve ser específico, informado e inequívoco, explícito na OS;

III. Implementar medidas de segurança técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, uso indevido, alteração, perda ou destruição: estas medidas incluem criptografia de dados, controle de acesso, treinamento de colaboradores e realização de auditorias de segurança;

IV. Limitar o acesso aos dados pessoais aos colaboradores que necessitem conhecê-los para o desempenho de suas funções: o acesso aos dados deve ser restrito ao mínimo necessário;

V. Não transferir dados pessoais para terceiros sem o consentimento do cliente, exceto nos casos previstos em lei: a empresa deve se certificar de que os terceiros com quem os dados são compartilhados também os protegem de forma adequada;

VI. Eliminar os dados pessoais quando não forem mais necessários para os fins para os quais foram coletados: a empresa deve estabelecer um procedimento para a eliminação segura dos dados pessoais;

VII. Atender às solicitações dos clientes de acesso, correção, exclusão, portabilidade, bloqueio ou oposição ao tratamento de seus dados pessoais: a empresa deve responder às solicitações dos clientes de forma tempestiva e eficaz;

VIII. Manter nomeado um Encarregado de Proteção de Dados (DPO): o DPO será responsável por garantir que a empresa esteja em conformidade com a LGPD.

8 Considerações Finais

Este documento demonstra, em linhas gerais, como os dados pessoais são coletados, tratados, usados, compartilhados, bem como as medidas adotadas para o tratamento dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares desses dados. Além disso, foram apresentadas informações que denotam o estágio atual de conformidade da Oliveira Filtros à LGPD.

Este Relatório será revisto e atualizado periodicamente ou sempre que a empresa implementar qualquer tipo de mudança que afete o tratamento dos dados pessoais. A Oliveira Filtros preocupa-se em avaliar continuamente os riscos de tratamento de dados pessoais que

surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

9 Aprovação

Responsável pela elaboração do Relatório de Impacto	Encarregado
Dr. Philipe Gustavo Portela Pires Advogado - OAB/SC 64.739 Mafra-SC, 5 de março de 2024	Dr. Jackson Alex Vinotti Advogado - OAB/SC 56.492 Mafra-SC, 5 de março de 2024

Autoridade representante do controlador	Autoridade representante do operador
Valceni Silveira de Oliveira Proprietário Mafra-SC, 5 de março de 2024	Não se aplica

GLOSSÁRIO

RIPD (Relatório de Impacto à Proteção de Dados Pessoais)	É a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD (Lei Geral de Proteção de Dados) e às liberdades civis e aos direitos fundamentais do titular de dados.
DIA (Data Impact Assessment):	Também conhecido como **Avaliação de Impacto à Proteção de Dados**, o DIA é um processo que visa avaliar os riscos e impactos do tratamento de dados pessoais em relação à privacidade dos titulares desses dados. Ele é especialmente relevante quando o tratamento envolve dados sensíveis ou de grande escala. O DIA ajuda a identificar e mitigar riscos, garantindo que o tratamento seja realizado de forma adequada e segura.
DIPIA (Data Protection Impact Assessment):	Em tradução representa **Avaliação de Impacto na Proteção de** Dados, trata-se de um processo sistemático para avaliar os riscos e impactos à privacidade decorrentes do tratamento de dados pessoais. O DIPIA é uma ferramenta importante para garantir a conformidade com a LGPD e proteger os direitos dos titulares dos dados.
LIA (Legitimate Interests Assessment):	O LIA, ou **Avaliação de Interesses Legítimos**, é um teste que deve ser realizado sempre que o controlador ou terceiro optar por justificar o tratamento de dados com base no legítimo interesse. Ele envolve verificar se o interesse da empresa em tratar os dados é lícito, adequado e proporcional, além de considerar outros fatores como a minimização dos dados e a existência de outras bases legais mais adequadas.
PIA (Privacy Impact Assessment):	O PIA, ou **Avaliação de Impacto à Privacidade**, é uma ferramenta que visa identificar e avaliar os riscos à privacidade decorrentes do tratamento de dados pessoais. Ele é aplicado em projetos, sistemas ou processos que envolvem dados sensíveis ou de grande escala. O PIA ajuda a tomar decisões informadas sobre como lidar com esses riscos e garantir a conformidade com a LGPD.
B2B (Business-to-Business):	Modelo de negócio que se concentra em transações comerciais entre empresas. Nesse contexto, as empresas atuam como tanto fornecedoras quanto clientes, comprando e vendendo produtos, serviços ou informações entre si, em vez de direcionar suas operações para o consumidor final. No ambiente B2B, as transações podem envolver uma ampla gama de produtos e serviços, desde matérias-primas e componentes industriais até soluções de software e consultoria empresarial. As empresas que operam no mercado B2B geralmente têm necessidades específicas e exigências mais complexas em

comparação com os consumidores individuais, o que pode influenciar a natureza das transações, os processos de vendas e os relacionamentos comerciais.

As transações B2B podem ocorrer por meio de diferentes canais, incluindo vendas diretas, distribuidores, marketplaces online, contratos de longo prazo e acordos de parceria. Essas transações são frequentemente caracterizadas por volumes maiores, ciclos de vendas mais longos e uma abordagem mais consultiva no processo de compra, onde a personalização e a customização dos produtos e serviços desempenham um papel fundamental.

O modelo B2B é essencial para o funcionamento de muitas cadeias de suprimentos e indústrias, desempenhando um papel vital na economia global ao facilitar o comércio e a colaboração entre empresas de diferentes setores e regiões.

Política de Segurança da Informação e Proteção de Dados (PSIPD)

Versão 1.0

Sumário

1 Introdução

O propósito deste documento é estabelecer e apresentar diretrizes de condutas adequadas da Segurança da Informação e Proteção de Dados da Oliveira Filtros.

A Política de Segurança da Informação e Proteção de Dados (PSIPD) estabelece as diretrizes para a adoção de procedimentos e mecanismos relacionados à segurança da informação e a boas práticas, de acordo com a NBR ISO/IEC 27002 - Código de Prática para a Gestão da Segurança da Informação e com a Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), visando orientar os colaboradores, fornecedores e demais que se relacionem com a Oliveira Filtros.

2 Objetivo

A Política de Segurança da Informação e Proteção de Dados (PSIPD) da Oliveira Filtros tem por objetivo instituir diretrizes estratégicas, mecanismos e controles que visam garantir atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos e armazenados, sob guarda ou transmitidos, por qualquer meio ou recurso, contra ameaças e vulnerabilidades.

Desse modo, a PSIPD busca preservar os ativos de informação, reduzir riscos de ocorrência de perdas e alterações desses, bem como de acessos indevidos a informações da Empresa e, sobretudo, preservar a imagem institucional da Oliveira Filtros. A finalidade desta Política é preservar as informações no que diz respeito à:

- **Confidencialidade:** somente pessoas devidamente autorizadas e que ratifique o AVISO DE PRIVACIDADE DE FUNCIONÁRIO e estejam capacitadas pela Empresa devem ter acesso à informação.
- **Integridade:** Somente alterações, supressões e adições autorizadas pela Empresa (e no caso da Lei 13.709/2018 – LGPD - consentidas pelo seu Titular) devem ser realizadas nas informações.
- **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas pela Empresa sempre que necessário ou demandado e no caso da Lei 13.709/2018 - LGPD consentidas pelo seu Titular.

3 Abrangência

A presente Política de Segurança da Informação e Proteção de Dados (PSIPD) alcança todos os processos que tratam ativos de informação da Oliveira Filtros, digitais e analógicos, que se relacionam à Empresa e os dados dos seus titulares.

Portanto, se aplica a todas as pessoas que trabalham na Oliveira Filtros, sejam colaboradores, estagiários, dirigentes, bem como a qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Empresa mantém relacionamento, dentre os quais: fornecedores, prestadores de serviço e clientes.

4 Referências

Esta Política foi desenvolvida tendo como suporte às seguintes normas:

- Norma ABNT NBR ISO/IEC Família 27000: Sistema de Gestão de Segurança da Informação (SGSI).
- Decreto-Lei nº 5.452, de 1º de maio de 1943: aprova a Consolidação das Leis do Trabalho (CLT).
- Lei Geral de Proteção de Dados Pessoais (LGPD): Lei nº 13.709/2018.
- Lei de Direitos Autorais: Lei nº 9.610/1998.
- Regulamento Interno de Segurança da Informação e Proteção de Dados (RISIPD).
- Código de Ética e Conduta.
- Política de Privacidade.
- Política de Cookies.

5 Diretrizes gerais

5.1 Proteção à Informação

As diretrizes de segurança da informação e proteção de dados estabelecidas nesta PSIPD se aplicam às informações originadas em papel e em meio digital, as convertidas para papel e meio digital, faladas, armazenadas, acessadas, produzidas, utilizadas, editadas, recebidas e transmitidas

pela Empresa. Essas diretrizes devem ser seguidas pelos usuários, os quais deverão atuar com responsabilidade e de acordo com o previsto nesta PSIPD.

Toda informação relacionada às operações da Empresa, gerada ou desenvolvida nas dependências da Empresa, físicas e virtuais, constitui ativo desta, independente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada.

A informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada e estritamente para o propósito institucional.

É diretriz que toda informação de propriedade da Empresa deva ser protegida de riscos e ameaças, que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade destas, através de medidas técnicas e administrativas tais como: perfil de acesso, controle de senhas, troca de senhas, armários com chaves, dentre outros.

Para consolidar a proteção da informação, garantir sua disponibilidade e segurança das informações tratadas, a Empresa, por meio das respectivas áreas responsáveis pelos procedimentos, sistemas, serviços e utilização destes, deve estabelecer, cumprir e fazer cumprir os procedimentos da PSIPD, do RISIPD e demais normativos internos

5.2 Confidencialidade de Dados e Informações

A Oliveira Filtros obriga-se a preservar a confidencialidade dos dados cadastrais e pessoais dos colaboradores, clientes, fornecedores, parceiros e conveniados, e os utilizará tão e somente para propósitos legítimos e específicos, de modo adequado e conforme as necessidades institucionais, utilizando-se das medidas técnicas e administrativas para proteger tais dados, de acordo com a presente Política de Privacidade da Empresa e pela Lei Geral de Proteção de Dados (LGPD).

São consideradas informações confidenciais, para os fins desta Política, as descritas no parágrafo anterior, bem como quaisquer informações não disponíveis ao público ou reservadas, tais como dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou

em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas para a Empresa.

O usuário que receber informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma, sob pena de se responsabilizar pelo seu uso indevido. Dados considerados sensíveis e de menores de idade devem ter atenção redobrada.

Nenhum dado ou informação confidencial pode ser compartilhado com terceiros, interna ou externamente à Empresa, sem consentimento por escrito do Controlador, sob pena de aplicação das sanções previstas nesta Política.

5.3 Responsabilidades

É missão e responsabilidade de cada colaborador, estagiário, dirigente, bem como de qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Oliveira Filtros mantém relacionamento: fornecedores, prestadores de serviço, clientes dentre outros, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente PSIPD.

É imprescindível que cada envolvido compreenda o papel da segurança da informação e proteção de dados pessoais em todas as suas atividades prestadas para a Oliveira Filtros, que devem respeitar a legislação vigente e a normatização proposta por órgãos e entidades reguladoras, com relação à segurança dos dados e informações.

É também obrigação de cada usuário se manter atualizado em relação a esta PSIPD e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso, tratamento e/ou descarte de informações.

Para auxiliar a todos os envolvidos, o Controlador é responsável por gerenciar as políticas e padrões que apoiam a todos na proteção dos ativos de informação e proteção de dados, além de auxiliar na resolução de problemas relacionados ao tema e disseminação do conteúdo desta PSIPD.

5.4 Descrumprimento e Sanções

As violações de segurança devem ser imediatamente informadas ao Controlador, as quais serão apuradas nos termos dos normativos internos, garantida a ampla defesa e contraditório de todos os envolvidos, com vistas à adoção das medidas necessárias, inclusive a correção da falha, se houver, ou reestruturação de processos.

O descumprimento das diretrizes desta PSIPD e a violação de normas derivadas da mesma sujeitam os envolvidos, além das sanções disciplinares cabíveis, inclusive à rescisão do contrato de trabalho, se colaborador for, e à eventual responsabilização civil e criminal.

6 Diretrizes específicas

6.1 Gestão de ativos

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho ou atividade, respeitando as recomendações técnicas, comportamentais e de sigilo específicas aplicáveis, constantes na **Política de Segurança e Privacidade (PPDP) da Oliveira Filtros**.

Como **condições gerais** para a gestão e o uso aceitável dos ativos de informação e dados dos titulares, esta PSIPD considera:

6.1.1 Acessos e Recursos de Rede

I. O acesso e o uso de todos os sistemas de informação, pastas de rede, bancos de dados e demais recursos (computadores, servidores de documentos e arquivos, impressoras, câmeras de vídeo, telefones, sistemas de videoconferência e audioconferência) devem ser restritos à pessoas expressamente autorizadas, de acordo com a necessidade para o cumprimento de suas atividades laborais e durante o exercício das mesmas nos ambientes da Oliveira Filtros (físicos ou virtuais) ou externas a ela.

II. O acesso a dados, informações, sistemas, serviços e redes, seja nos ambientes da Oliveira Filtros (físicos ou virtuais) ou externos a ela, via VPN, ou rede particular quando se aplicar, deve ser solicitado e/ou revogado conforme regras estabelecidas no PPDP da Oliveira Filtros.

III. Todo acesso será monitorado e se verificada a ocorrência de acessos desnecessários ou com poder excessivo, estes serão imediatamente revogados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

IV. Acessos fornecidos sob a forma de login (usuário e senha) seja para acesso à e-mail, sistemas, entre outros, sempre deverão ser realizados através de uso de senhas sigilosas. Senhas são de uso pessoal e intransferível, tendo sua divulgação e compartilhamento vedados sob qualquer hipótese, devendo ser alterada conforme as regras estabelecidas no PPDP.

V. A área técnica responsável da Oliveira Filtros poderá bloquear o login de qualquer usuário, no caso de suspeitas de vazamento de senhas ou de tentativas consecutivas de violação de acesso.

VI. Concessão e revogação de acessos para colaboradores, estagiários, dirigentes, bem como qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Oliveira Filtros mantém relacionamento: fornecedores, prestadores de serviço e clientes, terão suas regras descritas no PPDP.

6.1.2 Correio Eletrônico (e-mail) e Sistemas de Mensageria e de Correspondências

I. A Oliveira Filtros fornecerá, a seu critério exclusivo, o acesso às plataformas digitais e correio eletrônico (e-mail) ao colaborador, com o respectivo domínio, em sua admissão através de perfis de acessos previamente definidos, baseados em cargos e funções.

II. Por quaisquer meios de correio eletrônico, e-mail, mensageria e correspondência, o usuário é responsável pelas informações recebidas, enviadas e compartilhadas, bem como pela sua guarda, confidencialidade e publicidade.

III. As plataformas de colaboração, correio eletrônico e mensageria disponibilizadas pela Oliveira Filtros deverão ser utilizadas para fins corporativos e relacionados às atividades do colaborador, enquanto se mantiver o vínculo empregatício.

IV. As mensagens de correio eletrônico sempre deverão incluir assinatura conforme o padrão estabelecido pela Oliveira Filtros.

V. É obrigatória a manutenção da caixa de e-mails pelo respectivo usuário, evitando acúmulo de e-mails e arquivos desnecessários.

VI. O uso dos recursos de correio eletrônico, bem como o conteúdo das mensagens poderão ser vistoriados por amostragem, estando a Oliveira Filtros autorizada a ler, copiar, e/ou bloquear mensagens que violem as normas estabelecidas nesta PSIPD, no PPDP, Código de Ética e Conduta, e os interesses da Oliveira Filtros.

VII. É importante verificar o uso da ferramenta para que o envio de mensagens não seja caracterizado como SPAM, lixo eletrônico ou malware, abstendo-se de:

- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação.
- Produzir, transmitir ou divulgar mensagem que não estejam de acordo com a legislação vigente.
- Enviar mensagens contendo material protegido por direitos autorais sem a permissão do detentor dos direitos.
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas na legislação vigente ou ato normativo interno.

6.1.3 Internet (Rede Mundial)

I. Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet estará sujeita a divulgação e auditoria. Portanto, a Oliveira Filtros reserva-se o direito de monitorar e registrar todos os acessos à internet.

II. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Oliveira Filtros, que analisará e, se necessário, bloqueará qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em

unidade de armazenamento de dados local, na estação de trabalho, ou em áreas privadas da rede, visando assegurar o cumprimento desta PSIPD.

III. É proibido o acesso a sites da internet ou quaisquer arquivos digitais, bem como sua produção e propagação, que desrespeitem a Ética e os Bons Costumes, possuam conteúdo ilegal, pornográfico, preconceituoso, racista, bem como objetos, fatos, imagens, conceitos, opiniões e outros que possam disseminar o ódio e a violência e influenciar atitudes alheias aos interesses da Oliveira Filtros, expondo pessoas físicas ou jurídicas, produtos, marcas ou assemelhados à exposição pública, calúnia, injúria e/ou difamação.

6.1.4 Computação em Nuvem

O uso das "plataformas de nuvem" para transmissão e armazenamento de informações só poderá ocorrer nas plataformas formalmente contratadas pela Oliveira Filtros e disponibilizadas pela área técnica responsável.

6.1.5 Dados e Informações

I. A Oliveira Filtros preservará a confidencialidade dos dados cadastrais e pessoais dos seus titulares e os utilizará tão somente para propósitos legítimos e específicos, de modo adequado e conforme as necessidades institucionais, utilizando-se das medidas técnicas e administrativas aptas a proteger tais dados pessoais.

II. A Oliveira Filtros decidirá sobre o compartilhamento ou restrição de acesso aos dados e informações, sob sua gestão, bem como adotará meios de monitoramento do uso dos seus dados.

III. Cabe ao usuário da informação tratar as informações que estejam sob seus cuidados com zelo e de acordo com os princípios desta PSIPD e jamais, sob qualquer fundamento, tentar acessar informações e dados sem autorização para fazê-lo e sem correlação com suas funções laborais.

IV. Cabe ao usuário da informação documental proceder à guarda dos documentos que estejam sob seus cuidados em locais seguros durante o expediente, enquanto estiver manuseando e ao final do dia de trabalho.

V. Cabe à Oliveira Filtros adotar e manter Inventário de Dados e/ou Ativos de Informações, bem como os normativos internos relacionados.

VI. Cabe à Oliveira Filtros estabelecer condições para transferência segura de informações a partes externas, prevendo responsabilidades aos usuários que exercerem atividades de tratamento de dados pessoais, observando os seguintes processos:

- Controle e notificação de transmissões de dados pessoais.
- Procedimentos para assegurar a rastreabilidade dos eventos e o não repúdio.
- Notificação e registro de incidentes de segurança da informação, como perda de dados.
- Utilização de um sistema acordado de identificação para informações críticas e sensíveis, garantindo que a informação esteja devidamente protegida.

6.1.6 Guarda de Informações Digitais (Backup) e Documentação Física

I. Rotinas sistemáticas de backup e guarda de informações devem ser realizadas por colaboradores da área técnica responsável da Oliveira Filtros.

II. Cópias dos dados de produção, backup local e backup off-site devem ser produzidas, aplicando-se as melhores práticas de mercado com relação à segurança e proteção de dados.

III. Documentos imprescindíveis para as atividades da Oliveira Filtros deverão ser salvos em drives de rede corporativa, viabilizando a produção de backup e guarda da informação.

IV. Documentações Físicas devem ser guardadas/arquivadas de forma segura, quer seja em ambiente interno ou externo, de acordo com os prazos previstos em lei para guarda e arquivamento de referidos documentos.

V. As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um eventual desastre ocorrido no local principal, bem como as mídias de backup devem ser regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial.

6.1.7 Dispositivos de Impressão, Cópia e Digitalização

I. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis da Oliveira Filtros. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização. Ao usar uma impressora coletiva, o usuário deverá recolher o documento impresso imediatamente.

II. As impressoras e seus respectivos suprimentos são de uso exclusivo para as atividades da Oliveira Filtros.

III. Os usuários devem recolher imediatamente suas impressões, sejam elas corretas ou impressões com falhas. No caso de impressões com falhas, deverão ser descartadas de forma adequada.

IV. Impressões com falhas contendo informações sigilosas devem ser inutilizadas, tornando-as ilegíveis.

6.2 Gestão de Outros Recursos de Informação

6.2.1 Estação de Trabalho

I. Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não, devendo ser adequadamente armazenada em local provido com chaves/fechaduras.

II. No caso dos computadores, notebooks ou similares, os mesmos devem ficar bloqueados, mesmo quando o usuário se ausentar por curto período de tempo, assim como os dispositivos móveis, quando necessário, devem ser guardados em local provido com chaves/fechaduras.

III. Os usuários devem devolver todos os ativos de informação da organização que estejam em sua posse, após o encerramento de suas atividades, do respectivo contrato ou acordo.

IV. No caso de baixas patrimoniais ou uso do próprio equipamento pessoal pelo colaborador, deverão ser adotados procedimentos para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura do equipamento.

6.2.2 Controle de Acesso Físico

I. Todos os colaboradores da Oliveira Filtros que transitem por ambientes administrativos devem possuir identificação pessoal visível pelo uniforme da Empresa ou crachás contendo nome, foto, cargo e logomarca da Empresa.

8 Revisões

A Oliveira Filtros se reserva ao direito de revisar, adicionar ou modificar essa Norma de Segurança para aprimorar e garantir o perfeito funcionamento das regras por ela definidas. Essa revisão, adição ou modificação será notificada aos usuários com antecedência, exceto em situações emergenciais.

9 Termo de Ciência

O Termo de Aceite à PSIPD, deve ser assinado por todos os empregados e estagiários, devendo passar a constar, inclusive, como documento do processo de admissão ou de adaptação.

Os usuários devem entender os riscos associados ao aceite da PSIPD da Oliveira Filtros e cumprir rigorosamente o que está previsto neste documento.

Nos contratos em que se fizer necessário a concessão de acesso a ativos de informação da Oliveira Filtros, o aceite à PSIPD da Oliveira Filtros será condição imprescindível para que o tal acesso seja concedido, o que será instrumentalizado por intermédio de Termo de Aceite à PSIPD, contendo cláusula de Confidencialidade das informações.

Mafra, SC, 29 de abril de 2024.

VALCENI SILVEIRA DE OLIVEIRA ME
CNPJ n. 09.476.385/0001-32

POLÍTICA DE SEGURANÇA E PRIVACIDADE

OBJETIVO: A **OLIVEIRA FILTROS**, também popularmente conhecida como **CASA DOS FILTROS**, com o objetivo de demonstrar seu compromisso com a Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709/2018, assim como a segurança e privacidade dos dados pessoais dos seus clientes e parceiros, elaborou esta Política de Privacidade.

Você não é obrigado a compartilhar os Dados Pessoais que solicitamos, no entanto, se você optar por não os compartilhar, em alguns casos, não poderemos cumprir as finalidades descritas nesse documento.

MEDIDAS DE SEGURANÇA: As informações dos usuários serão armazenadas pela **OLIVEIRA FILTROS**, em servidores próprios ou de terceiros, contratados por esta, sempre protegidos por acordos de confidencialidade e seguindo todas as medidas de segurança exigidas por lei.

A **OLIVEIRA FILTROS** emprega os melhores esforços a fim de resguardar as informações dos usuários. Contudo, em razão da própria natureza da Internet, não há como assegurar que terceiros não autorizados não logrem sucesso em acessar indevidamente as informações armazenadas.

CONFIDENCIALIDADE DOS DADOS PESSOAIS COLETADOS: As informações coletadas são consideradas confidenciais e serão tratadas e armazenadas conforme as determinações desta Política e com a devida adoção das adequadas medidas de segurança.

DEFINIÇÕES:

LGPD (Lei Geral de Proteção de Dados)	A Lei nº 13.709/2018, que entrou em vigor em setembro de 2020 e dispõe sobre o tratamento de dados pessoais, inclusive meios digitais, realizado por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme art. 1º da LGPD.
OLIVEIRA FILTROS	**VALCENI SILVEIRA DE OLIVEIRA ME**, inscrita no CNPJ nº 09.476.385/0001-32, pessoa jurídica de direito privado, com sede na Rua Marechal Floriano Peixoto, 470. CENTRO I BAIXADA. MAFRA/SC. CEP: 89300-168.
Dados pessoais	Qualquer informação que possa identificar ou tornar identificável uma pessoa natural, conforme art. 1º da LGPD.

Titular	Pessoa natural a que se referem os dados pessoais que são objeto do tratamento, conforme art. 5º, inciso V, da LGPD.
Encarregado	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador/operador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

1. Organização Responsável pelo Tratamento: Todos os dados pessoais coletados na relação contratual são tratados exclusivamente pela **OLIVEIRA FILTROS**.

2. Dados Pessoais Tratados, Finalidades, Armazenamento e Prazo: A **OLIVEIRA FILTROS** poderá coletar Dados Pessoais e Dados Pessoais Sensíveis quando você acessa nosso site ou entra em contato conosco por qualquer meio de comunicação ou adquire nossos produtos, conforme demonstrado a seguir:

TIPOS DE DADOS	DADOS PESSOAIS	FINALIDADES DE USO DOS DADOS	PRAZO DE ARMAZENAMENTO	BASE LEGAL
ENTREGA E MANUTENÇÃO DOS PRODUTOS OFERECIDOS	E-mail; Nome, sobrenome, data de nascimento; Telefone e endereço.	Entrega e manutenção dos produtos vendidos e prestados pela Oliveira Filtros.	5 (cinco anos) a partir do cadastramento dos dados.	Interesse legítimo, conforme inciso IX, do art. 7º, da Lei n. 13.709/2018, a Lei Geral de Proteção de Dados (LGPD).
ENVIO DE E-MAIL E MARKETING	Nome, sobrenome, data de nascimento; Telefone e endereço; CPF/CNPJ; E-mail;	Enviar anúncios e ofertas, newsletter/e-mail marketing e comunicação da validade dos produtos.	5 (cinco anos) a partir do cadastramento dos dados.	Interesse legítimo, conforme inciso IX, do art. 7º, da Lei n. 13.709/2018, a Lei Geral de Proteção de Dados (LGPD).
DADOS PARA ANÁLISE DE CRÉDITO	Comprovação de renda; Nome e sobrenome; Análise de crédito.	Análise de Crédito.	Durante a relação contratual, incluso o prazo de garantia de 3 (três) meses contados da entrega do produto.	Proteção ao crédito, conforme inciso X, do art. 7º da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD).
RESPONDER A SOLICITAÇÃO DO TITULAR		Responder a solicitação do usuário;	Durante a relação contratual, incluso o prazo de garantia de 3 (três) meses contados da entrega do produto.	Interesse legítimo, conforme inciso VI, do art. 7º, da Lei n. 13.709/2018, a Lei Geral de Proteção de

				Dados (LGPD).
RECRUTAMENTO DE NOVOS COLABORADORES	Dados fornecidos no seu currículo.	Análise do processo seletivo ou admissional.	6 (seis) meses a partir do seu compartilhamento conosco ou durante a relação contratual.	Interesse legítimo, conforme inciso IX, do art. 7º, da Lei n. 13.709/2018, a Lei Geral de Proteção de Dados (LGPD).
COOKIES	Coleta de Cookies no site.	Aprimoração estratégica dos usuários dentro das nossas plataformas.	5 (cinco anos) a partir do cadastramento dos dados.	Interesse legítimo, conforme inciso IX, do art. 7º, da Lei n. 13.709/2018, a Lei Geral de Proteção de Dados (LGPD).

3. Crianças: Não coletamos conscientemente dados pessoais de crianças. Caso tomemos conhecimento de que coletamos os dados pessoais de uma criança e/ou adolescente, tomaremos medidas razoáveis para remover seus dados pessoais.

4. Com quem compartilharemos os dados: A **OLIVEIRA FILTROS** poderá compartilhar com provedores de serviços ou parceiros para gerenciar ou suportar certos aspectos de nossas operações comerciais em nosso nome, tais como prestadores de serviços de hospedagem e armazenamento de dados, gerenciamento de fraudes, vendas em nosso nome, atendimento de pedidos, personalização de conteúdo, atividades de publicidade e marketing (incluindo publicidade digital e personalizada), serviços de TI e com empresas afiliadas e parceiras de negócios a serviço da Oliveira Filtros para fins de conclusão de qualquer transação, de fornecimento das informações mais recentes sobre nossos produtos, serviços ou compartilhamento de nossas últimas promoções.

5. Direitos dos Titulares dos Dados: Conforme artigo 17 e seguintes da LGPD, a **OLIVEIRA FILTROS**, enquanto Controladora de Dados Pessoais, deverá garantir que os seguintes direitos dos titulares sejam garantidos.

- **Acesso aos Dados coletados e Confirmação da existência de tratamento:** todo titular dos dados tem direito de obter da **OLIVEIRA FILTROS** a confirmação de que seus dados são tratados, para quais finalidades e quais dados são estes.

- **Solicitação de Correção, Exclusão, Retificação, Transferência, Limitação, Oposição, Revogação de Consentimento, Informação das Entidades com quem houve compartilhamento de dados:** a qualquer momento o titular dos dados poderá exercer qualquer destes direitos, conforme aplicável, contatando o Encarregado, conforme item 6 deste documento.

6. Contato do Encarregado: Caso reste alguma dúvida sobre a presente Política ou em relação ao tratamento de dados pessoais, você poderá exercer seus direitos, entretanto em contato com o nosso Encarregado de Dados/ Data Protection Officer por meio do e-mail: casadosfiltrosmfa@gmail.com.

7. Como mantemos os dados seguros: Buscamos adotar as medidas técnicas e organizacionais previstas pelas Leis de Proteção de Dados adequadas para a proteção dos seus Dados Pessoais na **OLIVEIRA FILTROS**. Contudo, informamos que nenhuma transmissão ou sistema de armazenamento de dados tem a garantia de serem 100% seguros, de modo que, buscamos sempre evitar que vazamentos ocorram ao adotar um nível de proteção alto, realizando todos os testes de segurança necessários.

8. Mudanças na Política de Privacidade: Fica assegurado a **OLIVEIRA FILTROS** o direito de alterar a Política de Privacidade a qualquer momento, sem aviso prévio aos Titulares, de modo que é dever do Titular manter-se atento a possíveis atualizações dos referidos documentos, que serão imediatamente disponibilizados nos canais usualmente utilizados pela **OLIVEIRA FILTROS**, e as modificações entrarão em vigor na data da publicação da nova versão da Política de Privacidade.

9. Como ocorrerão as coletas automáticas de dados: De acordo com esta Política de Privacidade, nós podemos coletar seus Dados Pessoais de diversas formas, incluindo, mas não se limitando às seguintes:

Por meio do navegador ou dispositivos	Algumas informações são coletadas pela maior parte dos navegadores ou automaticamente por meio de dispositivos de acesso à Internet, como o tipo de computador, resolução da tela, nome e versão do sistema operacional, modelo e fabricante do dispositivo, idioma, tipo e versão do navegador de Internet que está utilizando. Podemos utilizar essas informações para assegurar

	que o Site funcione adequadamente.
Uso de Cookies	Informações sobre o seu uso do Site podem ser coletadas por terceiros, por meio de cookies. Cookies são informações armazenadas diretamente no computador que você está utilizando. Os cookies permitem a coleta de informações tais como tipo de navegador, o tempo despendido em sites, as páginas visitadas, as preferências de idioma, e outros dados de tráfego anônimos. Nós e nossos prestadores de serviço utilizamos informações para proteção de segurança, para facilitar a navegação, exibir informações de modo mais eficiente e personalizar sua experiência ao utilizar o site, assim como para rastreamento online. Também coletamos informações estatísticas sobre o uso do Site para aprimoramento contínuo do nosso design e funcionalidade, para entender como o Site é acessado e para auxiliá-lo a solucionar questões relativas ao site.

10. Leis e Foro aplicáveis: Essa Política de Privacidade será regida e interpretada de acordo com as leis da República Federativa do Brasil e as Partes elegem o Foro da Comarca de Mafra, Estado de Santa Catarina, como o único competente para dirimir qualquer litígio resultante desta Política de Privacidade.

VALCENI SILVEIRA DE OLIVEIRA ME
CNPJ nº 09.476.385/00013-2

POLÍTICA DE INCIDENTES DE DADOS (PID)
PLANO DE AÇÃO DE INCIDENTES DE DADOS (PAID)
PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS (PRISDP)

A **Oliveira Filtros** tem o compromisso de garantir a segurança e a privacidade dos seus dados pessoais. Acreditamos que a transparência é fundamental para construir uma relação de confiança com você, por isso, elaboramos esta Políticas e Panos de Incidentes visando sua segurança;

1. PID

1.1 Introdução

Esta Política e Planos se aplicam a todos os dados pessoais coletados pela **Oliveira Filtros**, tanto por meio de nossos canais físicos quanto digitais, incluindo:

- Website;
- Aplicativos;
- Redes sociais;
- E-commerce;
- Contato direto com a equipe de vendas ou atendimento ao cliente.

1.2 Incidentes de Segurança

Em caso de incidente de segurança que possa comprometer seus dados pessoais, a Oliveira Filtros tomará todas as medidas cabíveis para remediar a situação e minimizar os impactos, como:

- Notificação imediata aos órgãos competentes;
- Comunicação transparente com os titulares dos dados afetados;
- Adoção de medidas para mitigar os danos.

1.2.1 Categorias da violação de segurança

A violação de segurança será classificada dentre as categorias citadas a seguir:

a. Material: quando o incidente envolve dados armazenados em dispositivos físicos. Exemplos: perda de HD, pastas de arquivos perdidas, smartphones perdidos, etc.
b. Verbal: quando há vazamento de dados de forma verbal, seja por indiscrição (comentários acerca de dados pessoais que são percebidos por terceiros e utilizados em má-fé) ou de forma intencional, repassando indevidamente informações sigilosas.
c. Cyberespaço: quando o incidente está relacionado à Tecnologia da Informação. Nessa categoria enquadram-se o hackeamento, mau gerenciamento de patches, codificação incorreta, medidas de segurança insuficientes etc.

1.2.2 Avaliação da criticidade de segurança

Alguns fatores serão determinantes na definição da criticidade de um incidente:

I. A categoria da criticidade: de maneira genérica, o incidente será classificado em uma das categorias abaixo:
a. Risco Baixo: classificação utilizada quando o incidente de segurança de dados afetar apenas dados pessoais, não incluído o número do CPF;
b. Risco Moderado: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF, e/ou pelo menos um dado sensível, não incluído raça, religião, nome social e dados de saúde;
c. Risco Alto: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF e/ou mais que um dado sensível, incluindo raça, religião, nome social e dados de saúde.

II. Dados legíveis/ilegíveis: dados protegidos por algum sistema de pseudonimização (criptografia, por exemplo).

III. Volume de dados pessoais: expresso em quantidade de registros, arquivos, documentos e/ou em períodos de tempo (uma semana, um ano, etc.).

IV. Facilidade de identificação de indivíduos: facilidade com que se pode deduzir a identidade das pessoas a partir dos dados envolvidos no incidente.

V. Indivíduos com características especiais e criança e adolescente: se o incidente afeta pessoas com características ou necessidades especiais.

VI. Número de indivíduos afetados: dentro de uma determinada escala, por exemplo, mais de 100 indivíduos.

1.3 Colaboração em Investigações

A Oliveira Filtros se compromete a colaborar com as autoridades competentes em caso de investigações relacionadas a incidentes de segurança, fornecendo todas as informações e recursos necessários.

1.4 Notificação de Incidentes

É importante que qualquer agente que perceber algum possível incidente notifique a **Oliveira Filtros** imediatamente assim que identificar qualquer evento que possa colocar em risco a segurança de dados pessoais, como:

- Mensagens e e-mails suspeitos;
- Acessos não autorizados às contas e sistemas;
- Contato estranho que não seja por nossos canais oficiais ou agentes autorizados;
- Perda ou roubo de dispositivos.

1.5 Prevenção de Incidentes

A Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes essenciais para o tratamento de dados pessoais, visando garantir a privacidade e a segurança das informações dos cidadãos. Diante disso, é

imperativo que as organizações adotem medidas preventivas para evitar incidentes que possam comprometer a proteção desses dados.

Neste contexto, doutrinadores especializados têm contribuído com insights valiosos sobre as melhores práticas para prevenção de incidentes com dados pessoais, fornecendo orientações fundamentadas em sólida base teórica e prática.

Para prevenir incidentes de segurança, a Oliveira Filtros conta com a colaboração de todos os seus colaboradores, que devem:

- Estar atentos a qualquer atividade suspeita;
- Seguir as políticas de segurança da empresa;
- Reportar imediatamente qualquer incidente de segurança.

1.5.1 Ações para Prevenção de Incidentes com Dados Pessoais:

1.5.1.1 Implementação de Políticas Internas de Segurança de Dados:

"É fundamental que as organizações desenvolvam e implementem políticas internas robustas de segurança de dados, estabelecendo procedimentos claros e diretrizes específicas para o tratamento adequado das informações pessoais dos indivíduos." (Graça, 2020)

1.5.1.2 Treinamento e Conscientização dos Colaboradores:

"A capacitação contínua dos colaboradores é essencial para promover uma cultura de proteção de dados dentro das organizações. Os funcionários devem ser devidamente treinados e conscientizados sobre as boas práticas de segurança da informação e os procedimentos a serem seguidos para evitar incidentes com dados pessoais." (Silva, 2019)

1.5.1.3 Avaliação e Gerenciamento de Riscos:

"As organizações devem realizar avaliações periódicas de riscos relacionados ao tratamento de dados pessoais, identificando potenciais vulnerabilidades e ameaças à segurança da informação. Com base nessas análises, medidas preventivas e corretivas devem ser implementadas para mitigar os riscos identificados." (Almeida, 2021)

1.5.1.4 Utilização de Tecnologias de Proteção de Dados:

"A adoção de tecnologias avançadas de proteção de dados, como criptografia, controle de acesso e anonimização, é fundamental para garantir a integridade e a confidencialidade das informações pessoais dos usuários. Essas ferramentas auxiliam na prevenção de acessos não autorizados e na proteção contra-ataques cibernéticos." (Nascimento, 2018)

1.5.1.5 Monitoramento, registros e resposta a incidentes:

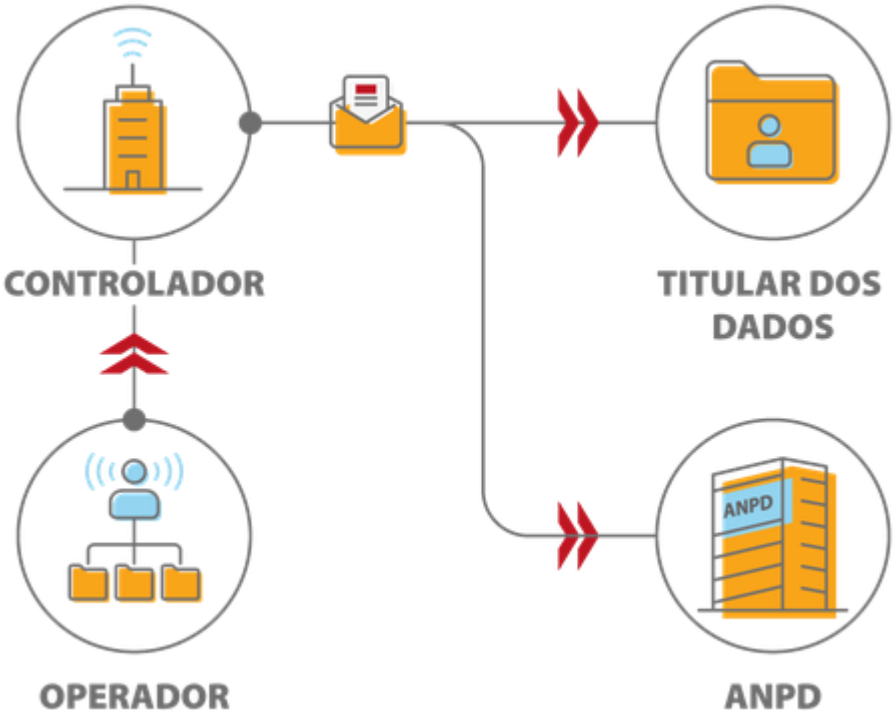
"É imprescindível que as organizações implementem sistemas eficazes de monitoramento e detecção de incidentes com dados pessoais, permitindo uma resposta rápida e eficiente em caso de violações

de segurança. Planos de contingência devem ser elaborados previamente, estabelecendo procedimentos claros para mitigar os impactos dos incidentes e garantir a conformidade com a LGPD." (Lima, 2020)

A prevenção de incidentes com dados pessoais é uma responsabilidade compartilhada entre as organizações e seus colaboradores, exigindo um compromisso contínuo com a proteção da privacidade e a segurança da informação.

O registro das atividades é importante para garantir a transparência nas operações com dados pessoais e a proteção dos direitos dos titulares dos dados. Além disso, ele permite que as autoridades regulatórias possam verificar se as atividades com dados pessoais estão sendo realizadas de acordo com as disposições da LGPD e tomar as medidas necessárias em caso de descumprimento da lei.

Ilustra-se brevemente para que seja mais bem compreendido, caso ocorra incidente de dados, qual o padrão a ser utilizado na comunicação:



Excepcionalmente, na hipótese de o controlador não dispor de informações completas a respeito do incidente ou não conseguir notificar a todos os titulares no prazo recomendado, a comunicação à ANPD poderá ser realizada em etapas: **preliminar e complementar**[1].

1.5.1.6 PRELIMINAR:

Entender quais são os dados e quais titulares foram afetados, isso pode ser feito cum uma análise simples das rotinas de tratamentos de dados, onde o operador irá explanar quais eram as informações contidas para que seja filtrada e separada essas informações de dados e titulares, de modo que se possa gerar um aviso de incidente em que se colocou em risco de vazamento. Dessa forma deve-se ser avisado pelo

[1] https://www.gov.br/anpd/pt-br/canais_atendimento/peticionamento-eletronico-anpd

contato registrado do titular que seus dados passaram por uma possível exposição e que estes devem ficar atentos, mesmo que não seja este titular efetivamente vítima do incidente.

1.5.1.7 COMPLEMENTAR:

Após mediada a primeira comunicação, controlador e operador deverão aprofundar as análises para interpretar os danos reais causados pelo incidente, adotando novas medidas e mais minuciosas para verificação real do ocorrido.

Assim, especificar quais dados foram acessados e de qual localização (ou aproximada) e se conseguiram definir para onde foram transferidos.

Também devem ser revelados aos titulares quais possíveis danos podem ocorrer em caso de uso dos dados por terceiros com intenções maliciosas, e quais as medidas básicas como: registro de boletim de ocorrência, verificação de logins e senhas, monitoramento de uso de CPF e aberturas de contas bancárias (através do Banco Central na ferramenta: https://registrato.bcb.gov.br/).

A impossibilidade de realizar a comunicação completa deve ser devidamente justificada pelo controlador. A complementação deverá ser encaminhada o mais breve possível e, no mais tardar, em 30 dias corridos contados da comunicação preliminar.

A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar, por meio de petição intercorrente.

1.5.2 Do prazo para comunicação de incidente

Qual o prazo para comunicar um incidente de segurança?

A lei determina que os incidentes de segurança devem ser comunicados aos titulares de dados e à Autoridade em prazo razoável, que foi definido pela Autoridade Nacional de Proteção de Dados (ANPD) em um regulamento próprio, sendo assim determinado que:

Para preservar os direitos dos titulares e tentar diminuir os possíveis prejuízos que um incidente de segurança possa causar, recomenda-se que **a comunicação seja feita o mais breve possível, em até 2 (dois) dias úteis da ciência do fato.**

A comunicação voluntária do incidente pelo controlador é demonstração de transparência, cooperação e boa-fé do agente e será considerada em eventual ação de fiscalização da ANPD.

Qual o papel do CONTROLADOR e do OPERADOR no processo de comunicação de incidentes de segurança?

A obrigação legal de comunicar o incidente de segurança aos titulares e à ANPD é do controlador, nos termos do art. 48 da LGPD. No entanto, a obrigação de adotar medidas para prevenir a

ocorrência de danos em virtude do tratamento de dados pessoais se estende a todos os agentes de tratamento de dados, inclusive aos operadores.

Quando um incidente de segurança ocorre, o operador deverá informar o fato, sem demora injustificada, ao controlador dos dados. Todas as informações necessárias à comunicação do incidente de segurança à ANPD e aos titulares deverão ser fornecidas pelo operador ao controlador.

A função do operador de dados, conforme prevista na Lei Geral de Proteção de Dados (LGPD), é garantir que todas as atividades realizadas com dados pessoais sejam realizadas de maneira a proteger a privacidade e os direitos dos titulares dos dados. Isso inclui desde a coleta, armazenamento, processamento, compartilhamento e destruição de dados pessoais.

O operador é responsável por garantir que todas as atividades relacionadas aos dados pessoais sejam realizadas de acordo com as disposições da LGPD, incluindo o cumprimento dos princípios de privacidade, transparência, finalidade limitada, adequação, minimização, exatidão, integridade e confidencialidade. Além disso, o operador também deve registrar todas as atividades que envolvam dados pessoais, incluindo as finalidades para as quais os dados são coletados, as fontes dos dados, as categorias de dados coletados, entre outros.

O registro das atividades é importante para garantir a transparência nas operações com dados pessoais e a proteção dos direitos dos titulares dos dados. Além disso, ele permite que as autoridades regulatórias possam verificar se as atividades com dados pessoais estão sendo realizadas de acordo com as disposições da LGPD e tomar as medidas necessárias em caso de descumprimento da lei.

Já adotando as ações sugeridas e seguindo as orientações da lei, dos doutrinadores especializados e do profissional que conduz a adequação, a **Oliveira Filtros** fortalece sua postura em conformidade com a LGPD e mitiga os riscos de incidentes com dados pessoais, garantindo a confiança dos indivíduos e o cumprimento das exigências legais.

Para o devido cumprimento da POLÍTICA DE INCIDENTES DE DADOS apresenta-se o PLANO DE INCIDENTES DE DADOS (PAID) e PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS (PRISDP) a seguir.

2. PAID E PRISDP

A PID recorre-se ao PAID para a necessidade de cumprimento do devido e estrito poder legal, mas também para a segurança de todos os usuários. Estes documentos contemplam e podem ser acionados em sua loja física e canais digitais para que o TITULAR obtenha respostas sobre incidentes qualificados com seus dados e seguirão as etapas ilustradas na figura abaixo e descritas na sequência:

Etapas da resposta a incidentes:

2.1 Antes do incidente

2.1.1 Planejamento

O planejamento consiste em identificar, prever e descrever possíveis situações de violação de dados, bem como as respectivas ações que deverão ser tomadas, os prazos e as formas de registro, garantindo que em situações reais se tenha um plano de ação previamente traçado. O planejamento deverá conter, no mínimo:

a) a previsão de possíveis situações de sinistros, bem como as formas de monitoramento e a ação que deverá ser tomada em caso de sua ocorrência;
b) a definição da área que deverá ser informada em situação de ocorrência do sinistro;
c) o detalhamento das ações necessárias deve levar em conta a criticidade do evento;
d) a criação de POLÍTICAS que estruturem a proteção de dados e privacidade que se encontram presentes no site: https://www.casadosfiltrosmafra.com/ ou no contato: dpo.oliveirafiltros@gmail.com

2.1.2 Identificação

Deve-se definir os critérios para detectar, identificar e registrar as situações de incidentes e descrever os recursos utilizados para a identificação de alertas de segurança e acionamento das equipes responsáveis para que sejam tomadas as devidas providências.

Devem ser avaliadas todas as possíveis fontes capazes de representar uma ameaça à proteção de dados, tais como:

a) recebimento de e-mail com anexos ou links suspeitos;
b) alteração no comportamento de equipamentos;
c) problemas ou lentidão no acesso a arquivos, sistemas ou serviços;
d) roubo, furto ou perda de equipamento que contenha informações;
e) vírus;
f) consumo excessivo de memória e/ou processamento;
g) tráfego de rede incomum;
h) conexões bloqueadas por firewall e
i) análise de logs e de desconformidade com as políticas internas da controladora.

Todos os colaboradores e prestadores de serviços são responsáveis por reportar qualquer tipo de evento e fragilidades que possam causar danos à segurança da informação, inclusive essas estarão nos registros, após identificadas pelos Operadores conforme art. 19, II e 37.

Dentro de nossa estruturação o nosso recurso de proteção técnico compreende etapas a serem cumpridas para casos de incidentes, conforme apresenta-se em cada caso. Contudo nosso roteiro de detalhamento em caso incidente é:

INCIDENTE - QUAL FATO GERADOR E DADOS FORAM PREJUDICADOS

↓

CRITICIDADE - QUAL A GRAVIDADE DOS DADOS QUE FORAM EXPOSTOS

↓

CATEGORIA - ONDE ENCONTRAVAM-SE ESTES DADOS
DIGITAL OU FÍSICO

↓

TIPO DE MONITORAMENTO - QUAL ANÁLISE E REGISTRO DE RESPONSÁVEIS E QUAL MODALIDADE

↓

A QUEM REPORTAR - TITULARES, ANPD, RESPONSÁVEIS LEGAIS, AUTORIDADE POLICIAL

↓

AÇÃO DE CONTENÇÃO - QUAL A MEDIDA PARA DIMINUIR E ENCERRAR O INCIDENTE

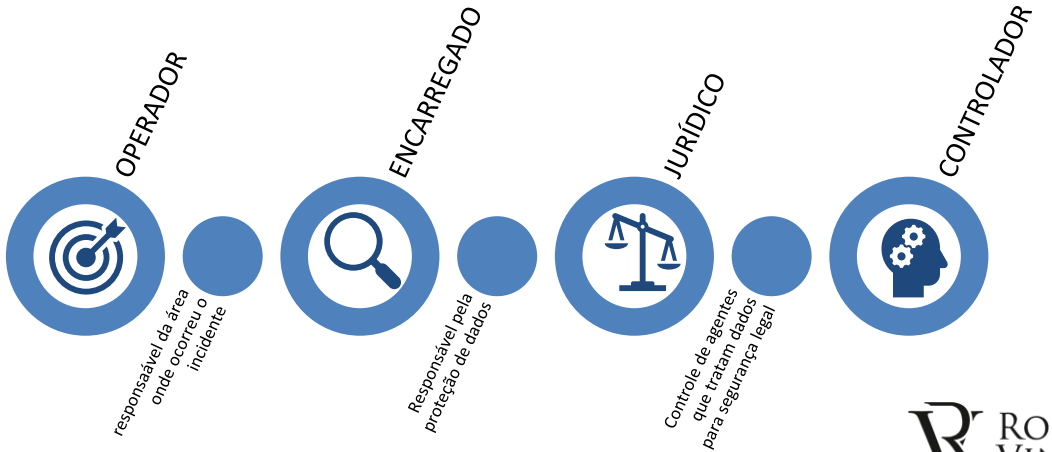
↓

AÇÃO DE ERRADICAÇÃO - COMO RASTREAR E/OU BLOQUEAR O DADOS DO INCIDENTE

2.2 Após o incidente

2.2.1 Contenção

Após um incidente ser identificado como uma violação de segurança, o mesmo deverá ser contido para evitar que outros sistemas sejam afetados ou que ocasionem danos maiores, deve ser previsto ações para a contenção de curto prazo, backup do sistema e contenção a longo prazo. Durante a contenção, deve haver o registro do incidente e das medidas de contenção que foram adotadas, evitando ao máximo a perda de evidências e as provas do ocorrido. É importante lembrar da necessidade de trabalho colaborativo de toda a Instituição, sobretudo dos membros destacados a seguir:



Após a identificação de um incidente, o mesmo deve ser contido e, se for o caso, isolado, para que outros sistemas/processos não sejam afetados, evitando maiores danos ao ambiente. Essa etapa inclui a contenção de curto prazo, backup do sistema, contenção a longo prazo, dentre outros.

É importante que, durante a etapa de contenção, ocorra simultaneamente a adoção de medidas que permitam a documentação e o registro do incidente, devendo ser evitado que evidências e provas do ocorrido sejam destruídas ou perdidas.

Nessa etapa, conforme a criticidade do incidente, poderão ser adotados os seguintes passos:

a) Desconectar o sistema/serviço comprometido ou isolar a rede afetada;
b) Alterar políticas de roteamento dos equipamentos da rede ou bloquear padrões de tráfego, interrompendo fluxo malicioso;
c) Desativar o sistema/serviço atingido para evitar maiores danos quando há perda ou roubo de informações;
d) Desabilitar sistemas/serviços vulneráveis para não comprometer outros sistemas/serviços;
e) Gerar backups dos sistemas/serviços não atingidos;
f) Verificar backups dos sistemas/serviços atingidos;
g) Envio de notificação/comunicação aos TITULARES de dados para ciência do incidente;

Obs.: A comunicação voluntária do incidente pelo controlador é demonstração de transparência, cooperação e boa-fé do agente e será considerada em eventual ação de fiscalização da ANPD.

2.2.2 Erradicação

Após o incidente ter sido contido, é necessário proceder com a sua correção e a restauração dos sistemas/processos que foram afetados, de modo que voltem a operar no seu estado anterior ao incidente.

Nesta etapa, a **Oliveira Filtros** precisa:

a) Analisar as causas do incidente;
b) Garantir que os métodos de acesso e as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente;
c) Providenciar a devida correção do ato gerador do incidente.

2.2.3 Recuperação

A recuperação é o conjunto de medidas visando restaurar os serviços de forma total, porém poderá ser realizada de forma gradual, conforme viabilidade e decisão do controlador.

Nesta etapa, a **Oliveira Filtros** precisa:

a) Iniciar o Plano de Continuidade de Negócio dos sistemas/serviços impactados;

b) Restaurar o sistema/serviço na íntegra;

c) Garantir que o sistema/serviço foi recuperado corretamente e que as funcionalidades estejam ativas;

d) Implementar medidas de segurança para evitar novos comprometimentos.

2.2.4 Revisão

Após o incidente contido e sua resolução encaminhada, a **Oliveira Filtros** através de sua equipe diretiva e responsáveis diretamente envolvidos deverá se reunir com o objetivo de discutir os problemas e dificuldades encontradas, propor melhorias/correções para os sistemas e processos e avaliar a eficácia deste Plano, bem como de suas Políticas.

Nesta etapa, a **Oliveira Filtros** precisa:

a) Identificar as características do incidente;

b) Reunir a equipe diretiva e responsáveis diretamente envolvidos para discussão do incidente;

c) Elaborar melhorias/correções em sistemas e processos envolvidos;

d) Prover, quando necessário, treinamento interno, visando a conscientização e a minimização de falhas;

2.3 Prazo e fundamento da comunicação

Seguindo o disposto no artigo 48 da referida Lei, **é obrigação do controlador comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares**. Devendo esta comunicação ser feita em prazo razoável, conforme definição da autoridade nacional, tendo em seu conteúdo, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos; A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata;
- As medidas que foram ou que estão sendo tomadas para reverter ou mitigar os efeitos do prejuízo.

Por isso conforme o item 1.5.2, o prazo da comunicação ser feita o mais breve possível, deve ocorrer em até 2 (dois) dias úteis da ciência do fato pelo controlador.

2.4 Fluxo da resposta a incidentes.

Responsável pelo tratamento de dados da área afetada pelo incidente: a partir do momento que foi identificado um possível incidente de segurança de dados, a área responsável pela categoria de dados deve imediatamente informar o encarregado de dados para iniciar o processo de contenção.

Operador: os operadores de dados, assim como os colaboradores internos, têm a responsabilidade de informar a ocorrência de incidente de segurança ao encarregado de dados, imediatamente.

Encarregado da Proteção de Dados: após ser informado, o encarregado de proteção de dados deverá avaliar a existência do plano de ação para tal incidente e iniciá-lo, e caso identifique o fato concreto de vazamento de dados pessoais, preencher o documento de Comunicação de Incidente de Segurança, para notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.

Jurídico: deve ser comunicada no intuito de auxiliar no processo de comunicação à ANPD e titulares de dados e tomar as medidas jurídicas cabíveis.

Tecnologia da Informação: será comunicada sempre que o incidente for relacionado a segurança da informação e que seja necessário medidas técnicas de tecnologia.

Administração: deve validar as medidas propostas no Plano de Respostas a Incidentes e oferecer subsídios para que elas sejam efetivamente cumpridas.

É fundamental que os mesmos erros não voltem a acontecer. Assim, é necessário que os incidentes sejam documentados, especificando quais foram os procedimentos de respostas utilizadas para contorná-los, de forma a manter um histórico das ocorrências e das ações tomadas.

TODAS AS POSSIBILIDADES QUE NÃO FOREM CONTEMPLADAS NESSE DOCUMENTO DEVEM SER DISCUTIDAS E ANALISADAS COM OS TITULARES, ENCARREGADO E CONTROLADOR.

Mafra/SC 07 de abril de 2024.

Responsável pela adequação: **PHILIPE PIRES**
Advogado, com inscrição na OAB/RS 113.682 | OAB/SC 64.739
especialista em Direito Digital e eletrônico, certificado em CDPP, DIA, DPIA CPA, LIA, PIA, DPO, LGPD e GDPR (Profissional em Proteção de Privacidade de Dados).

Encarregado (DPO): **JACKSON ALEX VINOTTI**
Advogado, com inscrição na OAB/SC 56.492 | OAB/PR 92.992
Rocha & Vinotti Advocacia - OAB/SC 6.589
CNPJ sob o n.º 41.982.838/0001-05, com sede na Av. Coronel José Severiano Maia, n.º 548, Vila Buenos Aires, Mafra/SC. CEP 89300-333

Os canais de comunicação referentes à LGPD são:
dpo.oliveirafiltros@gmail.com
rochaevinotti@gmail.com
dpo@philipepires.adv.br

VALCENI SILVEIRA DE OLIVEIRA ME
CNPJ nº 09.476.385/00013-2

CULTURA DE GOVERNANÇA E COMPLIANCE DE DADOS NA OLIVEIRA FILTROS

A cultura é uma estratégia de rotina a ser adotada por todos os colaboradores da empresa, medidas que devem servir para segurança própria e bem como dos dados de clientes e parceiros de prestação de serviços e fornecedores da **Oliveira Filtros**.

Prezado(a) colaborador(a) da Oliveira Filtros,

A **Oliveira Filtros** reafirma o compromisso com a integridade, segurança e ética no tratamento de dados, reconhecendo sua relevância para o sucesso de nossas operações. Com esse propósito, estamos implementando uma robusta **Cultura de Governança e Compliance de Dados**.

Esta iniciativa tem como objetivos primordiais:

1. **Proteger os dados pessoais** de nossos clientes, colaboradores, parceiros e demais stakeholders, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e demais normativas pertinentes.
2. **Garantir a confidencialidade**, integridade e disponibilidade dos dados, promovendo a qualidade e confiabilidade das informações utilizadas em nossas decisões.
3. **Promover a transparência** em nossas práticas de tratamento de dados, assegurando que os titulares estejam cientes de como suas informações são coletadas, utilizadas, armazenadas e compartilhadas.
4. **Fomentar a responsabilidade individual** e coletiva no tratamento de dados, sensibilizando todos os colaboradores sobre a importância da proteção de dados e da ética no manuseio da informação.

Para concretizar essa cultura, estamos adotando as seguintes medidas:

1. Constituição de um Comitê de Governança de Dados, composto pelos nossos sócios e, operador responsável e nosso Encarregado de dados, este grupo foi o responsável por estabelecer as políticas e diretrizes de governança e compliance de dados.
2. Elaboração de um abrangente Plano de Criação de Políticas de Proteção e de Compliance de Dados, delineando as ações a serem implementadas para garantir a conformidade com a LGPD e demais normativas pertinentes.
3. Realização de treinamentos e campanhas de conscientização destinados a todos os colaboradores, visando ressaltar a importância da proteção de dados e da conduta ética no uso da informação.
4. Estabelecimento de canais de comunicação para que os colaboradores possam reportar dúvidas, sugestões e incidentes relacionados à proteção de dados.
5. Implementação de medidas de segurança técnicas e administrativas para salvaguardar os dados contra acessos não autorizados, uso indevido, perda, alteração ou destruição.

Esta cultura está fundamentada nos seguintes princípios:

1. **Legalidade:** Todo tratamento de dados deve observar estritamente a legislação vigente.

2. **Transparência:** Os titulares dos dados devem ser informados de maneira clara e objetiva sobre o uso de suas informações.

3. **Segurança:** Os dados devem ser protegidos por meio de medidas adequadas contra ameaças internas e externas.

4. **Ética:** O tratamento de dados deve ser pautado pela ética e responsabilidade, respeitando os direitos e liberdades individuais.

5. **Responsabilidade:** Cada colaborador é responsável por zelar pela segurança e privacidade dos dados sob sua responsabilidade.

Nossas Políticas e Cultura de Governança e Compliance de Dados estão estabelecidas por tempo indeterminado e suas atualizações serão aplicadas e salvas com a especificação destacada em relatório público, constando da data de inclusão e exclusão de cada tópico.

Acreditamos firmemente que a adoção de uma Cultura de Governança e Compliance de Dados é essencial para atuação de cada membro da **Oliveira Filtros**.

Atenciosamente,

VALCENI SILVEIRA DE OLIVEIRA ME
CNPJ nº 09.476.385/00013-2

ACORDO DE PROCESSAMENTO DE DADOS (DPA)

OPERADOR: É denominada como **Oliveira Filtros** no Termo de Adesão à Prestação de Serviços celebrado entre as partes, a qual neste ato representada na forma de seu ato constitutivo; e;

CONTROLADOR: É denominada como **Cliente** no Termo de Adesão à Prestação de Serviços celebrado entre as partes, a qual neste ato representada na forma de seu ato constitutivo.

CONSIDERANDO QUE o **Controlador** deseja contratar os serviços ofertados pelo **Operador** e que, por conta disso, as Partes desejam implementar o presente Acordo de Processamento de Dados, a fim de atender às disposições legais aplicáveis à espécie, principalmente, no que tange à Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018).

De comum acordo, as partes acima qualificadas celebram o presente instrumento, que reger-se-á pelas disposições legais aplicáveis à espécie e termos e condições das cláusulas abaixo descritas, a saber:

CLÁUSULA 1º. GLOSSÁRIO

1.1 Os termos abaixo listados terão as seguintes definições:

i. Dados Pessoais	Toda informação relacionada a pessoa natural identificada ou identificável processada pelo **Operador** em nome do **Controlador** por conta do Contrato de Prestação de Serviços firmado;
ii. Titular dos Dados	Pessoa natural a quem os dados pessoais se referem;
iii. LGPD	Refere-se a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 de 2018);
vi. Controlador	A quem competem as decisões referentes ao **Tratamento de Dados**;
v. Operador	Realiza o **Tratamento de Dados** em nome do **Controlador**;
vi. Encarregado	Pessoa indicada pelo **Controlador** e **Operador** para atuar como canal de comunicação entre o **Controlador**, os titulares dos **Dados Pessoais** e a **Autoridade Nacional de Proteção de Dados – ANPD**;
vii. Transferência de dados	Refere-se aos **Dados Pessoais** obtidos pelo **Controlador** que são transferidos ao **Operador** em virtude do Contrato de Prestação de Serviços firmado. Ou ainda, refere-se à transferência autorizada dos **Dados Pessoais** aos terceiros pelo **Operador**, em observância aos requisitos legais aplicáveis à espécie;
viii. Tratamento de dados	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;

CLÁUSULA 2º. DO PROCESSAMENTO DOS DADOS PESSOAIS

2.1 Por meio do presente instrumento, o **Operador** declara e se obriga a: (i) Cumprir com todas as disposições previstas na **LGPD**; e, (ii) Não realizar o **Tratamento de Dados** em desacordo com as instruções dadas pelo **Controlador**.

2.2 De outro lado, por meio deste Acordo, o **Controlador** compromete-se a repassar todas as informações, orientações e todos os demais subsídios informacionais que o **Operador** necessite para realizar a atividade de **Tratamento de Dados**.

CLÁUSULA 3º. DA EQUIPE DO OPERADOR

3.1 O **Operador** tomará todas as medidas cabíveis para assegurar que todos os seus empregados, prestadores de serviço, prepostos, ou os terceiros que integram seu grupo econômico ou que venham a ter acesso às informações fornecidas pelo **Controlador**, terão acesso limitado às referidas informações, o qual será permitido apenas para o cumprimento de suas obrigações profissionais decorrentes da contratação celebrada.

3.2 Durante a vigência deste instrumento e após seu término ou rescisão, o **Operador**, seus empregados, prepostos, coligados e os terceiros, se obrigam a manter sob absoluto sigilo todas as informações comerciais, contábeis, administrativas e os **Dados Pessoais** revelados pelo **Controlador**, abstendo-se de utilizá-las em proveito próprio ou de terceiros.

CLÁUSULA 4º. DA TRANSFERÊNCIA DE DADOS

4.1 Os detalhes da **Transferência dos Dados** serão definidos entre os **Agentes de Tratamento** em conformidade com as Políticas de Segurança e Privacidade da Oliveira Filtros, via canais de comunicação mantidos entre eles.

CLÁUSULA 5º. DAS OBRIGAÇÕES

5.1 O **Controlador** declara e garante que:

a. O **Tratamento de Dados** é feito e permanecerá sendo feito de acordo com as disposições legais aplicáveis à espécie;

b. Instruirá o **Operador** para que o **Tratamento de Dados** seja realizado de acordo com as suas orientações e com as disposições previstas neste instrumento, bem como em respeito à legislação aplicável à espécie;

c. As medidas de segurança implementadas são apropriadas para proteger os **Dados Pessoais** coletados contra ataques ou perdas e/ou alterações acidentais, uso e/ou acesso não autorizado, e ainda contra todas as demais formas de **Tratamento de Dados** indevido, declarando e garantindo que as referidas medidas atribuem um nível apropriado de segurança contra os riscos inerentes ao desempenho das

atividades dos **Agentes de Tratamento**, levando-se em consideração os padrões esperados de segurança verificados no mercado;

d. Caso venha a ser necessário o compartilhamento de **Dados Pessoais**, obterá autorização para tanto;

e. Disponibilizará aos titulares dos **Dados Pessoais** que, eventualmente, sejam objeto de **Tratamento de Dados** uma cópia deste instrumento;

f. Em caso de compartilhamento de Dados Pessoais para realização do Tratamento de Dados, as medidas de segurança adotadas serão observadas da mesma forma;

g. Juntamente com o **Operador**, nomeará um **Encarregado** que será responsável por viabilizar a comunicação com os titulares dos **Dados Pessoais**, bem como com a **Autoridade Nacional de Proteção de Dados – ANPD**.

5.2 O **Operador** declara e garante que:

a. Irá realizar o **Tratamento de Dados** fornecidos pelo **Controlador** de acordo com as suas instruções, os termos previstos neste instrumento, bem como os dispositivos legais aplicáveis à espécie. Caso isso não seja possível, o **Operador** se prontificará a informar o **Controlador** de forma imediata.

b. Nenhuma das orientações repassadas pelo **Controlador** infringe a legislação aplicável à espécie, ou ainda as previsões constantes neste instrumento.

c. Possui uma organização técnica e de segurança capaz de atender as medidas solicitadas pelo **Controlador**.

d. Irá prontamente informar o **Controlador** acerca de: qualquer necessidade de repasse dos **Dados Pessoais** fornecidos às autoridades competentes, mediante solicitação oficial devidamente fundamentada; qualquer incidente com os **Dados Pessoais** fornecidos; ou de qualquer acesso não autorizado aos **Dados Pessoais** fornecidos;

e. Irá prontamente atender a qualquer questionamento feito pelo titular dos **Dados Pessoais** eventualmente repassados pelo **Controlador**, acatando prontamente às suas solicitações;

f. Irá prontamente atender a quaisquer requisições feitas pelas autoridades competentes mediante solicitação fundamentada;

g. Disponibilizará aos titulares dos **Dados Pessoais** que, eventualmente solicitem, uma cópia deste instrumento;

h. Se necessitar compartilhar os **Dados Pessoais** eventualmente fornecidos pelo **Controlador** com terceiros, irá solicitar sua autorização, bem como não medirá esforços para obter o consentimento prévio do titular;

i) Juntamente com o **Controlador**, nomeará um **Encarregado** que será responsável por viabilizar a comunicação com os titulares dos **Dados Pessoais** eventualmente repassados, bem como com a **Autoridade Nacional de Proteção de Dados – ANPD**.

CLÁUSULA 6º. DA RESPONSABILIZAÇÃO

6.1 As Partes acordam que, quando o **Controlador** compartilhar **Dados Pessoais** com o **Operador**, para fins de **Tratamento de Dados**, e ocorra qualquer evento que cause prejuízo ao titular dos **Dados Pessoais**, o **Controlador** se responsabilizará exclusivamente pela reparação ao titular.

6.1.1 O **Operador** somente se responsabilizará por ressarcir o titular dos **Dados Pessoais** compartilhados se o evento que tenha lhe causado prejuízos decorra de culpa exclusiva do **Operador** ou de seus colaboradores.

6.1.2 Se os prejuízos decorrerem de culpa concorrente do **Operador** e do **Controlador**, as Partes dividirão igualmente a responsabilidade de reparar o titular dos Dados Pessoais.

6.2. Se o **Operador**, sem ter incorrido em culpa, vier a ser acionado judicial ou administrativamente pelo titular dos **Dados Pessoais** eventualmente repassados pelo **Controlador**, este se prontificará a denunciar a lide e excluir o **Operador** do polo passivo da demanda, arcando com eventuais indenizações, multas, penalidades, custas judiciais, custas administrativas e honorários advocatícios incidentes eventualmente.

6.2.1. Se, por quaisquer motivos, não for possível a exclusão do **Operador**, e este vier a ser condenado a reparar o titular dos Dados Pessoais, o **Controlador** fica desde já obrigado a ressarcir o **Operador** por todos os custos que incorrer, sem prejuízo da reparação por eventuais perdas e danos.

CLÁUSULA 7º. DO COMPARTILHAMENTO DE DADOS

7.1 Para prestar os seus **Serviços** ou vender seus produtos em favor do **Controlador**, o **Operador** deverá compartilhar os **Dados Pessoais** fornecidos com os colaboradores da empresa, sob pena de inviabilizar-se a prestação.

7.1.1 Por meio do presente instrumento, o **Controlador** autoriza o compartilhamento dos **Dados Pessoais** fornecidos ao **Operador**.

7.1.2 Caso o **Operador** necessite compartilhar os **Dados Pessoais** fornecidos pelo **Controlador** com terceiro, não será necessário requisitar autorização prévia ao **Controlador.**

7.2 O **Operador** celebrará instrumentos particulares com cada um dos terceiros que guardem relação comercial, impondo o cumprimento das mesmas obrigações previstas neste **Acordo**, fazendo com que todos os terceiros listados observem as medidas de segurança de **Dados Pessoais** repassadas pelo **Controlador** ao **Operador.**

7.2.1 Se, por quaisquer motivos, o **Operador** não conseguir garantir que os terceiros atendam as medidas de segurança referidas acima, informará ao **Controlador** que decidirá se será possível prosseguir ou não com o **Tratamento de Dados**, responsabilizando-se perante os titulares dos **Dados Pessoais** eventualmente compartilhados.

7.3 Se qualquer um dos terceiros inobservarem as orientações do **Controlador** repassadas pelo **Operador**, serão responsáveis pelo ressarcimento do **Controlador** e/ou do **Operador** e/ou do titular dos **Dados Pessoais**, sem prejuízo da parte prejudicada buscar indenização suplementar pelas perdas e danos experimentados.

7.4 O **Operador** manterá a listagem dos terceiros com quem compartilha os **Dados Pessoais** repassados pelo **Controlador** atualizada, disponibilizando o livre acesso a consultas a serem realizadas pelo **Controlador**.

CLÁUSULA 8º. DA COOPERAÇÃO COM AS AUTORIDADES

8.1 O **Controlador** aceita disponibilizar uma cópia deste instrumento às autoridades competentes mediante requisição legalmente fundamentada de acordo com a legislação aplicável à espécie.

8.2 As partes concordam que a **Autoridade Nacional de Proteção de Dados – ANPD**, mediante requisição legalmente fundamentada de acordo com a legislação aplicável à espécie, poderá auditar os dados em posse do **Controlador**, do **Operador** e dos terceiros que mantêm relação.

CLÁUSULA 9. DO TÉRMINO DO TRATAMENTO DOS DADOS

9.1 As Partes acordam que, salvo disposição legal em sentido contrário, quando do término do **Tratamento de Dados**, ou quando se for atingida a finalidade dos **Serviços** ofertados, ou ainda quando o **Tratamento de Dados** se mostrar insuficiente para se atingir às finalidades pretendidas, o **Operador,** e os terceiros, irão devolver tais **Dados Pessoais,** e suas respectivas cópias e registros, ao **Controlador**. Alternativamente, o **Operador,** e os terceiros, poderão destruir os **Dados Pessoais** fornecidos pelo **Controlador.**

CLÁUSULA 10. DAS DISPOSIÇÕES GERAIS

10.1 O presente instrumento traduz a integral vontade das Partes e substitui todo e qualquer outro ajuste, convenção, ou entendimento, verbal ou escrito, firmado entre as mesmas anteriormente, desde que diga respeito ao objeto deste instrumento, os quais, com sua assinatura, perdem neste ato toda sua validade e eficácia, sendo substituído pelo presente contrato, único documento válido que consubstancia os recíprocos direitos e obrigações das partes.

10.2 A tolerância por qualquer das partes em relação ao descumprimento de quaisquer das disposições contidas neste instrumento não significará, em momento algum ou sob qualquer hipótese, renúncia aos direitos referentes a tais disposições, não afetará, sob qualquer pretexto, a validade deste instrumento, no todo ou em parte, e nem obstará o direito da parte prejudicada de exigir o cumprimento de toda e qualquer obrigação devida pela parte faltosa.

10.3 A invalidade, ineficácia ou inexequibilidade de quaisquer das disposições contidas neste instrumento não invalidará nem tornará ineficaz ou inexequível quaisquer das demais disposições nele previstas, as quais continuarão em pleno vigor, comprometendo-se as partes a negociar e envidar seus melhores esforços para acordarem as medidas necessárias para sanar tais disposições de eventuais vícios.

10.4 O presente instrumento poderá ser reformado ou emendado, em qualquer tempo, por mútuo consenso das partes, desde que através de instrumento escrito revestido das mesmas formalidades do presente.

10.5 O presente instrumento é celebrado em caráter irrevogável e irretratável, obrigando não só as partes como também seus sucessores a qualquer título.

10.7 As partes declaram e concordam que o presente instrumento constitui título executivo extrajudicial.

CLÁUSULA 11. DO FORO

11.1 O presente instrumento deverá ser interpretado de acordo com a legislação vigente na República Federativa do Brasil, ficando eleito o Foro da Comarca de Mafra/SC, para dirimir judicialmente as controvérsias decorrentes do pactuado por meio do presente instrumento.

CLÁUSULA 12. DO ACEITE

12.1. Para validação deste acordo, considerará a concordância por assinatura ou aceite eletrônico através de Ordem de Serviço ou confirmação de compra pelo cliente, o qual estará em pleno acordo com as Políticas da empresa e termos deste documento.

VALCENI SILVEIRA DE OLIVEIRA ME
CNPJ nº 09.476.385/00013-2