Edição	Histórico das Publicações	Elaborado	Verificado	Aprovado
MAI/24	Versão 01. Procedimento novo Versão 02. Revisão	Shirley Peixoto	Comitê	Daniel Borba

A Política de Segurança da Informação é um conjunto de regras internas que abrange a segurança, proteção e confidencialidade, e serve como guia para orientar e disciplinar colaboradores e terceiros. O documento aborda o atendimento à Lei Geral de Proteção de Dados entre outros assuntos importantes ao sistema de Compliance.

1) OBJETIVOS:

Essa política tem por objetivo assegurar os requisitos da Lei Geral de Proteção de Dados, por meio de diretrizes que orientam colaboradores, parceiros, fornecedores, clientes e terceiros, no que diz respeito a segurança da informação, visando ainda, complementar as definições contidas no código de conduta do Grupo Vertical em vigor, além do cumprimento das legislações e obrigações legais de proteção e integridade de dados.

O Grupo Vertical obedece a todos os deveres e obrigações contidas na Lei Geral de Proteção de Dados e Segurança da Informação, e preza por respeito à privacidade, inviolabilidade da intimidade, da honra e da imagem, desenvolvimento econômico e tecnológico e inovação, livre iniciativa, livre concorrência e a defesa do consumidor, bem como dos direitos humanos, livre desenvolvimento da personalidade, da dignidade e o exercício da cidadania pelas pessoas naturais.

2) REVISÃO E DIVULGAÇÃO

A presente política será revisada anualmente, devendo ser aprovada pelo Comitê de Segurança de Informação, como garantia de atendimento à legislação e/ou qualquer alteração de rotinas.

A qualquer tempo, conforme necessidade, poderão ocorrer alterações, em conformidade com as normas eu regulam o tratamento de dados, o que deverá ser informado pelo demandante de forma expressa para o setor de Compliance (responsável pela manutenção do Sistema de Informação), que, em conjunto com todos os envolvidos fará a alteração necessária e informará.

A divulgação após a revisão anual será comunicada a todos, de forma eletrônica, desde a alta direção, colaboradores, prestadores de serviços e demais interessados e envolvidos no negócio, garantindo a evidência do recebimento e ciência da nova versão do documento.

Em caso de revisão anterior ao marco anual definido, todos os envolvidos serão devidamente informados com a garantia de evidência do envio/recebimento do fato comunicado.

3) COMPROMETIMENTO:

Art. 50

Termo de Confidencialidade Assinado por Todos

4) CONCEITOS GERAIS:

Dados Pessoais: São todas as informações pessoais do titular, que possam identificar a pessoa natural.

Dados sensíveis: De acordo com o Regulamento Geral sobre a Proteção de Dados, dados sensíveis são dados vinculados à pessoa natural, dos quais possuam origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico capazes de causar qualquer tipo de discriminação. Por esse motivo, merecem maior atenção e proteção especial por meio dos usuários desses dados.

Dado anonimizado: Dado referente a titular que não possa ou não queira ser identificado, considerando a utilização de meios razoáveis e disponíveis para o devido seu tratamento.

Banco de dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

5) TRATAMENTO DE DADOS PESSOAIS

(De acordo com o art. 7º, incisos I ao X, e caput art. 23)

O tratamento de dados no Grupo Vertical obedece aos requisitos mencionados nos arts. art. 7º e Art. 23 da Lei 13.709/2018, que aborda os Requisitos gerais para o tratamento de dados pessoais, bem como as hipóteses em que pode ocorrer o uso/tratamento de dados pessoais, que compreende os eventos abaixo:

Para o cumprimento de obrigação legal ou regulatória;
Pela administração pública, para a execução de políticas públicas, incluindo o tratamento e uso compartilhado de dados;
Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular;
Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
Para a proteção da vida ou da segurança física do titular ou de terceiros;
Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
Quando necessário para atender ao legítimo interesse do controlador ou de terceiros;
Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente; e
Atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências ou cumprir as atribuições legais do serviço judicial.

6) COMO SÃO TRATADOS PELO GRUPO VERTICAL

O Grupo Vertical realiza o tratamento de dados de clientes o qual possui vínculo de venda de mercadoria para realização de cirurgias. Assim, os tratamentos realizados são somente coleta, armazenamento, transmissão interna entre os setores responsáveis pelo processo, conclusão de processo, faturamento e arquivamento.

Coleta: O acesso às informações deve ser sempre ocorrer por meio de sistemas informatizados ou por canal de comunicação seguro e formalizado, de forma anonimizado. Este procedimento visa diminuir o risco de acesso à dados pessoais e sensíveis desnecessariamente.

O referido acesso somente é realizado para utilização individualizada, de acordo com a solicitação do material, não sendo realizada quaisquer alterações nas informações coletadas.

Cadastro: Após finalização da cotação, os dados da solicitação deverão ser cadastrados no sistema VM System, local em que é realizado todo o processo de acompanhamento para separação de produto pelo setor de logística, andamento, conclusão e faturamento.

Armazenamento: O armazenamento de documentos e dados é realizado no sistema VM System, onde é realizada toda a tramitação do processo de venda.

Obs.: O prazo para armazenamento dos dados no e-mail será de até 2 anos após o orçamento, após o término do tratamento estes serão descartados e excluídos. Já o armazenamento no Sistema Informatizado VM obedecerá ao prazo estabelecido em lei especial.

Descarte: Os dados pessoais, em consonância com a legislação, ao concluir sua finalidade, são descartados, exceto se necessário cumprimento de obrigação legal ou regulatória. Para os demais dados, o descarte ocorre em: 5 anos para dados relativos à gestão de pagamento ou de controle de horas remuneradas; – 20 anos para dados referentes a um registro médico; – 3 anos para informações de contato de um cliente potencial que não respondeu a nenhuma solicitação; – 6 meses para dados de registro (log).

Outra forma de descarte, é realizada após a conclusão do processo de faturamento e fiscalização interna. Completado o processo de tratamento de dados pessoais, o auxiliar ou analista de cada setor realizará o descarte dos dados (quando for dados digitais) e os documentos físicos, deverão ser encaminhados ao arquivo geral, que realizará o processo de incineração.

Compartilhamento: O compartilhamento de dados poderá ocorrer diante de situações em que ocorreram reclamações de materiais que apresentam defeito de fabricação e no recebimento dos produtos que não estão em conformidade com a qualidade. Assim, é realizado o procedimento descrito no Procedimento – POP 30, (Reclamações de Produtos), o qual será compartilhado os dados apenas com as empresas responsáveis pelo ocorrido (Fornecedores vinculados ao Grupo Vertical), bem como para a Agência Nacional de Proteção de Dados (ANPD).

Obs.: Toda a tramitação de dados é realizada por meio do sistema interno VM system, para acompanhamento e conclusão do processo para a empresa, não sendo permitida nenhuma modificação ou alteração sem autorização, com exceção do compartilhamento externo com os fornecedores.

Todo o tratamento interno de dados deverá observar a confidencialidade, sendo restrita somente aos usuários legítimos. Qualquer transferência externa deverá ser realizada mediante **autorização prévia do setor de Compliance**, além de conter registro, suporte, a data, a hora, o remetente e o número de unidades incluídas na remessa, o tipo de informação, a forma de remessa e as pessoas responsáveis pelo recebimento ou entrega.

5.1) TIPO DE DADOS COLETADOS:

O Grupo Vertical poderá coletar os dados interessados durante a realização do serviço de cotação e compra de material, com identificação em sistema próprio para a finalidade que se destina, conforme exemplos citados a seguir. (Razão Social, CNPJ, Inscrição Estadual, contato, e-mail, etc.)

Informações de contato: inclui qualquer tipo de dado de contato: nome, endereço residencial, endereço eletrônico (e-mail), números de telefone, perfil em redes social etc.

Informações demográficas: inclui informações sobre dados demográficos, como data de nascimento, idade ou faixa etária, gênero, localização geográfica.

Informações de Prontuários: Conjunto de documentos que apresenta o histórico de atendimentos condição de saúde de pacientes.

Informações técnicas: inclui informações sobre seus equipamentos computacionais ou dispositivos móveis, como: registro do endereço IP utilizado para conectar seu computador ou dispositivo à internet, incluindo sua localização geográfica, tipo de sistema operacional e do navegador da web.

Informações financeiras e de pagamento: sobre serviços utilizados referentes a produtos fornecidos, coleta dados financeiros e de pagamento para o seu processamento em conformidade com as leis, normas e os padrões de segurança aplicáveis para a prestação do serviço.

7) AGENTES E COMPETÊNCIAS

(De acordo com o art. 37 ao art. 40 da Lei 13.709/2018)

Controlador: pode ser uma pessoa natural ou pessoa jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, ou seja, o controlador é responsável pelo tratamento dos dados. O Controlador tem, entre outras, as seguintes competências previstas na LGPD:

- Manter registro das operações de tratamento de dados pessoais;
- Elaborar relatório de impacto à proteção de dados pessoais, inclusive dados sensíveis, relativo ao tratamento de dados;
- Orientar o operador quanto ao tratamento de dados segundo instruções internas, da legislação vigente e das regulamentações da Autoridade Nacional de Proteção de Dados (ANPD).

Co controlador: Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome e por ordem do controlador. No Grupo Vertical, operador é a pessoa natural ou jurídica, de direito público ou privado, externa ao quadro funcional, que realiza o tratamento de dados pessoais em nome e por ordem do controlador.

Encarregado: Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

De acordo com a LGPD, o Encarregado é responsável por:

- Receber as reclamações e comunicações dos titulares
- Responder e adotar providências;
- Receber as comunicações da ANPD e adotar as providências necessárias;
- Orientar todos os colaboradores da instituição sobre as práticas a serem tomadas em relação à proteção de dados pessoais
- Realizar treinamentos periódicos internamente.
- Executar outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares estabelecidas pela ANPD.

7) BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

(De acordo com o art. 7º, incisos I ao X, e caput art. 23)

O tratamento de dados pessoais pelo Grupo Vertical poderá ser realizado sem o termo de consentimento, por se tratar de dados pessoas referentes à saúde, assegurado pelos fundamentos a seguir:

- Para o cumprimento de obrigação legal ou regulatória;
- Pela administração pública, para a execução de políticas públicas, incluindo o tratamento e uso compartilhado de dados;
- Para a realização de estudos por órgão de pesquisa, via anonimização dos dados pessoais, sempre que possível;
- Quando necessário para a execução de contrato ou de procedimentos relacionados a contrato do qual seja parte o titular;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Para a proteção da vida ou da segurança física do titular ou de terceiros;
- Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Quando necessário para atender ao legítimo interesse do controlador ou de terceiros;
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente; e
- Atendimento de sua finalidade com o objetivo de executar as competências ou cumprir as atribuições legais do serviço de distribuição de materiais.

Haverá legítimo interesse do Grupo Vertical como Operador de dados, de acordo com a presente base legal para tratamento de dados pessoais em situações de apoio às suas atividades ou, ainda, a proteção do exercício regular de seus direitos ou da prestação de serviços que o beneficiem a saúde do titular, respeitados os direitos e liberdades fundamentais do titular dos dados.

7.1) DO CONSENTIMENTO: (De acordo com o art. 8º da LGPD)

O consentimento referente à coleta de dados do usuário deverá ser obtido de forma livre, expressa, individual, clara, específica e legítima e poderá ser revogado a qualquer momento pelo usuário. Será dispensado para o tratamento de dados pessoais para o exercício do direito à saúde, sendo realizado e observado de acordo com a finalidade, a boa-fé, resguardados os direitos do titular.

O Consentimento na área da saúde fica dispensado, de acordo com as exceções previstas em Lei. (*De acordo com o art. 7º, incisos I ao X, e caput art. 23*)

Diante disso, o usuário poderá solicitar a exclusão dos dados utilizados em tratamentos a qualquer momento, o qual poderá encerrar o cumprimento dos serviços relacionados a essa base legal, por meio de preenchimento do formulário de pedido no acesso pelo usuário no sistema informatizado Power Automate.

7.2) DA FINALIDADE (De acordo com o art. 9º)

A coleta de dados tem por finalidade atuar de forma eficaz e proporcionar a entrega exata de materiais solicitados aos seus destinatários ou usuários, relativos aos serviços oferecidos pelo Grupo Vertical.

- O tratamento de dados pessoais tem por finalidade a prestação dos serviços de distribuição de materiais para realização de cirurgias e produtos dietéticos.
- A maior parte dos dados é extraída das informações enviadas por meio de comunicação informatizado de solicitações médicas (para a realização de cirurgias), ou por fornecimento do titular, para a mesma finalidade. Esses dados serão usados exclusivamente para atender as solicitações enviadas ao Grupo Vertical, de modo a agilizar e cumprir integralmente a entrega dos materiais.
- Caso ocorram mudanças da finalidade para o tratamento de dados pessoais, não compatíveis com o consentimento original, o titular será informado previamente, garantido o direito de revogar o consentimento, se discordar das alterações.

7.3) DIREITOS DOS USUÁRIOS

(De acordo com o art. 17 a 22 da LGPD)

O titular dos dados pessoais poderá a qualquer tempo, por meio de requisição específica, obter informações sobre o tratamento de seus dados pessoais perante o Grupo Vertical, garantidos os seguintes direitos:

- Livre acesso, facilitado e gratuito (acesso pelo PowerAutomate)
- Confirmar existência, acessar, revisar, retificar, e/ou requisitar uma cópia eletrônica da informação dos seus dados pessoais (este deverá comprovar sua autenticidade) – 15 dias para resposta
- Requisitar detalhes sobre a origem ou o compartilhamento com terceiros (solicitação pelo PowerAutomate)
- Limitar o uso e divulgação de seus dados pessoais;
- Solicitar a anonimização, bloqueio, eliminação, portabilidade e oposição de seus dados pessoais;
- Revogar o consentimento, excetuando-se as situações previstas na legislação, e receber informações sobre as consequências do não consentimento ao uso de seus dados pessoais.

Os requisitos da Política de Segurança da Informação devem ser cumpridos por todos o qual o Grupo Vertical possui relacionamento, no entanto, em casos de violação, alteração, exclusão ou outras solicitações referentes ao devido tratamento de dados pessoais, o titular poderá demandar seu interesse por meio do sistema informatizado, através do preenchimento e solicitação no site (Power Automate).

Prazo: A solicitação é respondida em até 15 dias contados da solicitação pelo titular, de acordo com a Lei Geral de Proteção de Dados.

8) SOLICITAÇÕES E RECLAMAÇÕES GERAIS

(De acordo com art. 09,18 e 19 da LGPD)

9) TRATAMENTO DE DADOS SENSÍVEIS

(De acordo com o art. 11 da LGPD)

O Grupo Vertical realiza o tratamento de dados sensíveis por se tratar de dados compartilhados pelo Controlador. Desta forma, o Grupo tem acesso às informações referentes à gênero, situação de saúde e outros, de forma à atender especialidades de acordo com cada procedimento médico realizado.

- Por se tratar de dados sensíveis referentes à saúde, e não haver consentimento o Grupo Vertical deverá obedecer às políticas de segurança e privacidade, bem como firmar termo de confidencialidade e sigilo de informação.

10) TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

(De acordo com o art. 14 da LGPD)

O Grupo Vertical se preocupa com a proteção de direitos de crianças e adolescentes, bem como se preocupa com o tratamento de dados pessoais de crianças e de adolescentes com a finalidade de atender o seu melhor interesse, o qual só poderá ser realizado com o consentimento expresso dos pais ou responsável legal, com a específica finalidade do tratamento.

- O Grupo Vertical manterá sigilo das informações fornecidas pelo titular e seu representante legal.

11) DO TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS

(De acordo com o art. 15 e 16 da LGPD)

De acordo com a LGPD, o término do tratamento de dados pessoais pelo Grupo Vertical ocorrerá nas seguintes hipóteses:

- Verificação de que a finalidade foi alcançada, ou de que os dados deixaram de ser necessários para alcance da finalidade almejada;
- Fim do período de tratamento;

- Solicitação de revogação pelo titular, resguardado o interesse público.
- Determinação pela autoridade nacional, quando houver violação à proteção de dados pessoais.

O Grupo Vertical realiza o tratamento de dados pessoais pelo tempo necessário a cumprir a finalidade pelos quais foram coletados, de acordo com sua base legal. Quando do término do tratamento, os dados pessoais serão eliminados de sistemas como e-mails, sendo autorizada o armazenamento nas situações previstas em legislações vigentes.

12) POLÍTICA DE COOKIES E COMO SÃO TRADADOS

Cookies são arquivos criados por meio de protocolos usados em navegadores do usuário ao visitar um site. Os cookies são utilizados para garantir o bom funcionamento de sites e demais serviços online, assim como para fornecer informações sobre o endereço IP, tipo de navegador, sistema operacional, páginas visitadas, duração da visita. Entretanto, se o usuário recusar o uso de cookies, nem todos os recursos de navegação no site e nos serviços poderão ser acessados.

O Grupo Vertical só realiza coleta de dados mediante consentimento informatizado de cookies por meio de navegadores dos usuários, clientes, colaboradores, prestadores e fornecedores que possuem relacionamento, bem como dar publicidade da política de cookies para evidenciar a negação da presente prática. O site do Grupo Vertical emite comunicado o(a) usuário(a) antes do usuário aceitar a política de cookies e permite que o usuário estabeleça sua vontade de recusá-los.

13) Compartilhamento de dados internamente

O compartilhamento externo de dados e dados sensíveis é proibido por parte do Grupo Vertical, sendo permitido somente nos casos previstos no presente código. O compartilhamento interno de dados, é realizado entre a cadeia de setores do Grupo Vertical, com o objetivo de troca e acompanhamento de informações pertinentes aos processos dos seguintes setores:

- Recursos Humanos
- Compliance
- Cotação
- Qualidade
- Financeiro
- Contabilidade
- Fiscal
- Logística

É vedado aos colaboradores, prestadores e parceiros comerciais compartilhar ou divulgar informações e imagens internas, por qualquer meio e forma com terceiros não vinculadas ao grupo, conforme termo de sigilo e confidencialidade assinado.

De acordo com o Código de Conduta do Grupo Vertical, no item “Sistema de Informação e Mídias Sociais”, é também vedado publicações ou divulgação de conteúdo nas redes sociais. A utilização ou publicações indevidas podem resultar em consequências negativas, como em violação de dados pessoais.

14) MONITORAMENTO DE CÂMERA DE PROTEÇÃO

O Grupo Vertical utiliza câmeras de vídeo para segurança, a este tratamento é dispensada a obrigação de consentimento, pois possui apenas a finalidade de proteção da vida, integridade física da empresa, colaboradores e terceiros. O uso das imagens deve cumprir estritamente esta finalidade. Ressalta-se que as câmeras externas realizam apenas a proteção em volta da unidade da empresa e não realiza o monitoramento de áreas públicas.

Consultar Norma SI.01-4

15) DIVULGAÇÃO LEGAL DOS DADOS

A divulgação de dados realizada pelo Grupo Vertical, somente será realizada em casos de solicitação pela Agência Nacional de Proteção de Dados, bem como por interesse do titular dos dados ou por cumprimento legal. Não haverá qualquer outra divulgação de dados pessoais sem os casos previstos na presente política.

16) SEGURANÇA DE DISPOSITIVOS E DOCUMENTOS:

O Grupo Vertical visa facilitar o processo interno quanto às informações, e se preocupa em preservar os ativos da empresa.

Consultar Normas SI.01 – 4, 6

17) MEDIDAS DE SEGURANÇA – TELA LIMPA

O Grupo Vertical realiza a segurança de equipamentos e computadores objetiva assegurar a autenticidade do uso, e se preocupa com a integridade dos ativos e privacidade de dos dados internos. Desta forma, é necessária a adoção de algumas medidas para prevenir que dados ficam desprotegidos no ambiente de trabalho quando em uso ou não:

O Grupo Vertical utiliza documentação física e digital, a fim de facilitar o manuseio e processos internos. Assim, torna-se obrigatório a responsabilidade de proteção adequada destes por todo o Grupo adequada. O objetivo da segurança de documentação e dispositivos é garantir a integridade dos ativos utilizados diariamente, assim como evitar pane, desastres, extravio, edição, alteração e exclusão indevidas entre outros.

Consultar Manual de Segurança da Informação

18) AUDITORIA

O Setor de Compliance realiza auditorias internas, com o objetivo de verificar se todos os processos, atividades, controles, atendimento a legislação e demais elementos, e visa buscar conformidades. As auditorias internas realizadas na empresa possuem periodicidade anual sendo realizada por colaboradores treinados para a realização de auditorias de Compliance, esta analisa as políticas/procedimentos, registros e controles realizados e evidências, bem como estabelece as recomendações de melhoria para o sistema ou emite não conformidades.

20) DA VIOLAÇÃO DE DADOS PELO GRUPO VERTICAL:

(De acordo com art. 42 da LGPD)

Em casos de vazamento/violação de dados o controlador deverá emitir medidas cabíveis para fazer cessar a violação. Se da violação ocorrer dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais a outrem, a empresa é obrigada a repará-lo. A reparação.

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados

21) COMUNICAÇÃO

CONSCIENTIZAÇÃO E TREINAMENTO:

Todos os colaboradores deverão receber um treinamento sobre a Segurança da Informação, abordando a evolução da implantação da LGPD e Segurança da Informação na empresa, as disposições contidas na Política de Segurança da Informação e apresentação de demais medidas de proteção. Quando há alteração das políticas descritas, toda a empresa precisa realizar novo treinamento, bem como seus parceiros comerciais informados e todos devem ter acesso à política atualizada. Se não houver alterações no código os colaboradores devem ser treinados bienalmente sobre as políticas contidas no código.

Sigilo:

Toda e qualquer informação interna é protegida por sigilo industrial, não podendo em hipótese alguma ser divulgada, compartilhada ou relatada externamente sem o expresso consentimento da empresa. Este sigilo atinge igualmente as informações relacionada aos colaboradores e clientes da empresa.

Complementa esta Política os seguintes documentos:

Manual do Sistema de Informações
Normas SI.01 de 01 a 09