

POLÍTICA DE GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS DO GRUPO SOMA

Esta política foi atualizada em 30 de abril de 2022

OBJETIVOS

O GRUPO SOMA está comprometido com a proteção dos dados e a preservação da privacidade dos Titulares. Esta Política se aplica ao Tratamento de Dados Pessoais realizado pelo GRUPO SOMA e tem como principais objetivos:

- Assegurar a conformidade do GRUPO SOMA com as leis e regulamentações aplicáveis à proteção de Dados Pessoais;
- Proteger os direitos dos Colaboradores, clientes, fornecedores, parceiros ou qualquer pessoa natural que tenha seus Dados Pessoais tratados pelo GRUPO SOMA, bem como reforçar a confiança perante estes Titulares;
- Ser transparente com relação aos procedimentos do GRUPO SOMA no Tratamento de Dados Pessoais; e
- Promover a conscientização em relação à proteção de Dados Pessoais e questões de privacidade, difundindo a cultura de privacidade e proteção de dados no GRUPO SOMA.

1. A QUEM SE APLICA

Esta Política se aplica tanto ao GRUPO SOMA quanto às suas subsidiárias, diretas ou indiretas, salvo na existência de política específica ou documento equivalente aprovado sobre o tema previsto nesta Política no que se refere a essas sociedades.

2. DEFINIÇÕES

Para os efeitos desta Política, as seguintes definições terão os significados assinalados abaixo:

- a) **Bases Legais:** hipóteses legais que autorizam o Tratamento de Dados Pessoais, especialmente as previstas nos artigos 7º e 11 da Lei nº 13.709/2018.
- b) **Lei Geral de Proteção de Dados Pessoais (LGPD):** Lei nº 13.709/2018.
- c) **Dados Pessoais:** informação relacionada a pessoa natural identificada ou identificável (p. ex., nome, número de identificação, endereço IP, voz, fotografia, dados de localização etc.).
- d) **Dados Sensíveis:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- e) **Tratamento de Dados Pessoais:** toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- f) **Controlador:** pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de Dados Pessoais. Pode ser o GRUPO SOMA.
- g) **Operador:** pessoa natural ou jurídica que realiza o Tratamento de Dados Pessoais em nome do Controlador.
- h) **Encarregado de Proteção de Dados:** pessoa indicada pelo Controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.
- i) **Autoridade Nacional de Proteção de Dados (ANPD):** Autoridade responsável pela supervisão do cumprimento das regras sobre proteção de Dados Pessoais no Brasil.
- j) **Incidente:** violação de segurança que provoque, de modo acidental ou ilícito, destruição, perda, alteração, divulgação, bloqueio ou acesso, não autorizados, a Dados Pessoais tratados.
- k) **Titular:** qualquer pessoa natural identificada ou identificável, cujos Dados Pessoais são tratados.

- l) **Política:** Documento interno que dispõe as ações, comportamentos e procedimentos que precisam ser seguidos dentro de uma empresa. Elas refletem o propósito e os objetivos de uma organização e estabelecem o que deve ser feito para alcançá-los.
- m) **Record of Processing Activity – ROPA:** Registro de Atividades de Processamento realizado para o mapeamento de atividades envolvidas no tratamento de dados pessoais.
- n) **Programa de Governança ou Programa:** programa de governança em privacidade e proteção de dados implementado e constantemente atualizado e avaliado pelo GRUPO SOMA, bem como formalizado pela presente Política para adequação do GRUPO SOMA à LGPD.
- o) **Colaboradores:** sócios, diretores, administradores, empregados, prestadores de serviços, parceiros e/ou quaisquer outros similares.
- p) **Companhia ou GRUPO SOMA:** Grupo de Moda Soma S.A e suas subsidiárias.

3. DOCUMENTOS DE PROTEÇÃO DE DADOS

Abaixo, estão descritos e brevemente explicados as políticas e os procedimentos de privacidade e proteção de dados pessoais empregados no contexto do programa de governança do GRUPO SOMA, de acordo com a LGPD, que devem ser considerados em conjunto com esta Política:

- a) **Regimento Interno do Comitê de Privacidade:** O GRUPO SOMA instituiu o Comitê e Sub Comitê de Privacidade com intuito de reforçar o compromisso com valores éticos e morais já adotados pela organização e para o fiel cumprimento da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD). O Comitê e Sub Comitê são formados observando as diretrizes do Regimento Interno do Grupo e dispõe de uma estrutura organizacional composta por profissionais comprometidos, qualificados, que conhecem os valores, os propósitos e a missão da organização.
- b) **Escritório de Privacidade:** O GRUPO SOMA possui o Escritório de Privacidade com a finalidade de promover as ações necessárias com vistas ao cumprimento

das disposições da Lei Geral de Proteção de Dados (LGPD), de nº 13.709. Com natureza permanente, consultivo-deliberativa, tem a responsabilidade estratégica de articular as ações necessárias para a gestão e proteção de dados pessoais, atendendo às áreas que tratam dados pessoais, os prazos legais estipulados e assegurando a continuidade da Governança no GRUPO SOMA.

- c) **Política de Privacidade:** O GRUPO SOMA possui uma Política de Privacidade que tem por objetivo estabelecer as diretrizes e regras para garantir a segurança dos dados pessoais tratados pelo GRUPO SOMA em conformidade com a Lei 13.709/18.
- d) **Política de Segurança da Informação:** O GRUPO SOMA preza pela segurança da informação que trata durante a execução das suas atividades, de modo que tem uma Política de Segurança da Informação, que estabelece as diretrizes corporativas do GRUPO SOMA para a proteção dos ativos de informação e a prevenção de danos.
- e) **Aviso de Privacidade:** : O GRUPO SOMA tem três documentos de transparência, que descrevem, entre outros pontos, os tipos de dados pessoais tratados e as finalidades para as quais são tratados pelo GRUPO SOMA, conforme exigido pela LGPD. São eles o Aviso de Privacidade do GRUPO SOMA – para clientes, revendedores e influenciadores, o Aviso de Privacidade de Candidatos às vagas do GRUPO SOMA e o Aviso de Privacidade para Colaboradores do GRUPO SOMA.
- f) **Procedimento de Contratação de Fornecedores:** O GRUPO SOMA tem um procedimento que traz orientações sobre como os Colaboradores devem proceder quando houver contratação de fornecedores cuja prestação de serviços envolva o Tratamento de Dados Pessoais, visando minimizar riscos e avaliar o nível de adequação dos terceiros com os quais o GRUPO SOMA se relaciona.
- g) **Modelos de Cláusula de Proteção de Dados do GRUPO SOMA:** O GRUPO SOMA tem modelos de cláusula de proteção de dados – que variam de acordo com a posição das partes no Tratamento de Dados Pessoais e o volume de Dados Pessoais tratados – que devem ser utilizados na adequação da relação com terceiros cuja contratação envolve o Tratamento de Dados Pessoais.

- h) **Procedimento de Registro de Processamento (ROPA):** O GRUPO SOMA tem, conforme exigido pela legislação, o registro das atividades de tratamento de dados pessoais, por meio de uma Plataforma com detalhamento dos dados pessoais tratados, a categoria dos Titulares envolvidos na atividade e a Base Legal que legitima este Tratamento. O Registro deverá ser constantemente atualizado.
- i) **Procedimento de Retenção e Descarte de Dados Pessoais:** O GRUPO SOMA tem um procedimento com regras sobre como proceder em relação à retenção e ao descarte de arquivos (físicos ou digitais) e informações que contenham dados pessoais, visando à integridade dos sistemas, a privacidade e a proteção dos Dados Pessoais das pessoas físicas que se relacionam com o GRUPO SOMA.
- j) **Procedimento de atendimento dos direitos dos titulares:** O GRUPO SOMA possui procedimento detalhado que tem por objetivo apresentar o passo a passo para atendimento das solicitações dos Titulares de Dados previsto na Lei Geral de Proteção de Dados Pessoais - Lei 13.709/2018 ("LGPD") e orientar os Colaboradores e Parceiros de Negócio do GRUPO SOMA quanto aos seus papéis e responsabilidades.
- k) **Plano de Resposta a Incidentes:** O GRUPO SOMA elaborou uma estratégia de como agir em caso de quebra de confidencialidade, integridade ou disponibilidade dos dados pessoais. O plano define as ações a serem tomadas desde a identificação do Incidente até a sua documentação e posterior treinamento, para que não ocorra novamente.
- l) **Template de Relatório de Impacto à Proteção de Dados Pessoais:** O GRUPO SOMA tem um *template* de Relatório de Impacto à Proteção de Dados para avaliar os processos de tratamento de dados pessoais que podem trazer algum risco para os titulares. O preenchimento desse documento ajuda os colaboradores do GRUPO SOMA a analisarem os processos mais críticos das suas respectivas áreas e a indicarem medidas de mitigação de riscos necessárias para o Tratamento dos dados envolvidos nesses casos.
- m) **Template de Teste de Legítimo Interesse:** O GRUPO SOMA tem um *template* de avaliação de legítimo interesse, de forma a garantir que – quando o

tratamento se fundamentar nessa base legal – todos os requisitos legais aplicáveis a essa base sejam cumpridos.

- n) **Questionário *Privacy by Design*:** No GRUPO SOMA, todo novo processo ou produto é pensado considerando a proteção de dados, os princípios da LGPD e o exercício dos direitos dos titulares desde a sua concepção. Assim, o GRUPO SOMA tem um questionário que ajuda os Colaboradores a identificarem se novos processos ou produtos estão de acordo com a LGPD.
- o) **Treinamento e Conscientização:** O GRUPO SOMA possui um plano de treinamento e conscientização para todos os colaboradores da organização e, quando relevante, os contratados deverão receber educação e treinamento de conscientização adequada e atualizações regulares nas políticas e procedimentos organizacionais, conforme relevante para sua função de trabalho.

4. ESCOPO

Esta Política deverá ser observada em conjunto com as demais políticas do GRUPO SOMA, incluindo as indicadas no acima, em todas as atividades de Tratamento de Dados Pessoais. A presente Política deve ser observada por todas as áreas e marcas do GRUPO SOMA, bem como por todos os Colaboradores que, no âmbito dessa relação, tratem Dados Pessoais.

5. PRINCÍPIOS

Ao realizar o Tratamento de Dados Pessoais, o GRUPO SOMA e seus Colaboradores devem atentar-se aos seguintes princípios:

- a) **Finalidade:** coleta de Dados Pessoais apenas para fins legítimos, específicos, explícitos e informados ao Titular, sem a possibilidade de Tratamento posterior de forma incompatível com essas finalidades.
- b) **Adequação:** compatibilidade do Tratamento dos Dados Pessoais com as finalidades informadas ao Titular, de acordo com o contexto do Tratamento.

- c) **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 informadas ao Titular.
- d) **Livre acesso:** 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.
- e) **Qualidade dos dados:** garantia de que os Dados Pessoais tratados são precisos e atualizados.
- f) **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.
- g) **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de Incidentes.
- h) **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais.
- i) **Não discriminação:** impossibilidade de realização do Tratamento para fins discriminatórios ilícitos ou abusivos.
- j) **Responsabilização e prestação de contas:** demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Esses princípios devem nortear todas as atividades de tratamento de Dados Pessoais desenvolvidas pelo GRUPO SOMA, incluindo a criação de novos produtos ou serviços. Ao criar ou revisar processos que envolvam o tratamento de Dados Pessoais, os Colaboradores devem verificar a lista dos dez princípios e certificar-se de que estes estão sendo contemplados em todo o ciclo de vida do dado – da coleta ao descarte.

6. BASES LEGAIS

O GRUPO SOMA somente poderá tratar Dados Pessoais caso exista uma Base Legal que permita o Tratamento do Dado Pessoal. Assim, antes de realizar qualquer atividade

de Tratamento, a Base Legal correta precisa ser identificada e indicada no Registro de Atividades de Tratamento de Dados Pessoais do GRUPO SOMA.

Caso seja identificado qualquer tratamento de dados pessoais pelo GRUPO SOMA sem a devida Base Legal, tal tratamento deve ser interrompido e os dados – caso não sirvam a outras atividades de tratamento legítimas – eliminados. Caso haja dúvidas em relação a este procedimento, o Colaborador deve entrar em contato com o canal indicado ao final da Política.

Considerando as atividades do GRUPO SOMA, o Tratamento de Dados Pessoais ou Dados Sensíveis pelo GRUPO SOMA deve ser sempre amparado em uma Base Legal. Abaixo, são indicadas as mais prováveis de serem aplicáveis às atividades de Tratamento do GRUPO SOMA.

Base legal	Detalhamento
<p>Legítimo interesse do GRUPO SOMA ou de terceiros</p> <p><i>(não aplicável a Dados Sensíveis)</i></p>	<p>Essa hipótese é bastante ampla e contempla casos em que, diante de uma situação concreta, o GRUPO SOMA verifica que (i) tem uma finalidade lícita para uso dos dados; (ii) há uma expectativa do Titular em ter seus Dados Pessoais tratados no contexto analisado.</p> <p>Essa Base Legal não pode ser utilizada quando prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos Dados Pessoais. Para avaliação dos requisitos acima listados o GRUPO SOMA tem um modelo de teste de legítimo interesse.</p>
<p>Execução de contrato do qual seja parte o Titular, ou procedimentos preliminares para formação do contrato, a pedido do Titular</p> <p><i>(não aplicável a Dados Sensíveis)</i></p>	<p>Essa hipótese se aplica quando há um contrato firmado entre o GRUPO SOMA e o Titular (pessoa física) e a atividade de Tratamento é essencial ao objeto do contrato ou à formação do contrato.</p> <p>Exemplificativamente, é possível indicar a necessidade de tratamento (i) dos dados</p>

	<p>bancários dos empregados pelo GRUPO SOMA, pois é preciso realizar o pagamento da remuneração; e (ii) de dados como o endereço do cliente para entrega de produtos, pois é necessário entregar o produto para finalizar a compra.</p>
<p>Consentimento</p>	<p>O consentimento é a autorização dada pela próprio Titular para o Tratamento dos Dados Pessoais. Essa autorização deve ser:</p> <ul style="list-style-type: none"> a) <u>Livre</u>: o Titular deve ter a opção de negar o consentimento sem que tenha consequências negativas que extrapolem a não realização do Tratamento; b) <u>Informada</u>: o Titular deve ter clareza do propósito de uso dos Dados Pessoais, de qual é a empresa responsável (Controlador) e dos demais elementos essenciais para a tomada da decisão; c) <u>Inequívoca</u>: o consentimento não pode ser implícito e depende de uma ação afirmativa do Titular. <i>Check-box</i> pré-marcado, por exemplo, não configura uma ação inequívoca do Titular. <p>O consentimento, quando viável, é especialmente recomendado para viabilizar o Tratamento de Dados Sensíveis. Nesse caso, o consentimento deve também ser <u>destacado</u>.</p> <p>Adicionalmente, em regra, os dados de crianças (Titulares menores de 12 anos) só podem ser tratados mediante a coleta de consentimento – além dos requisitos acima indicados – específico e em destaque dos responsáveis.</p>

<p>Cumprimento de obrigação legal ou regulatória</p>	<p>É a Base Legal adequada para Tratar Dados Pessoais quando o Controlador é obrigado, por lei ou outras normas, a fazê-lo. É, por exemplo, o caso do Tratamento necessário à emissão de notas fiscais ou à coleta, pelo GRUPO SOMA, de Atestado de Saúde Ocupacional (ASO) dos Colaboradores.</p>
<p>Exercício regular de direitos em processo judicial, administrativo ou arbitral <i>(não aplicável a Dados Sensíveis)</i></p>	<p>É a Base Legal utilizada para que o GRUPO SOMA possa atuar em processos. Trata-se da hipótese adequada para embasar as atividades necessárias para reunir provas, apresentar documentos no âmbito do processo etc.</p>
<p>Proteção da vida ou da incolumidade física do Titular</p>	<p>É a Base Legal adequada para Tratar Dados Pessoais quando há um risco à vida do Titular.</p>
<p>Exercício regular de direitos, pelo GRUPO SOMA, Titular ou Terceiro, inclusive em contrato e em processo judicial, administrativo e arbitral <i>(Exclusiva para casos de tratamento de Dados Sensíveis)</i></p>	<p>É a Base Legal que autoriza o uso de Dados Sensíveis quando o Controlador, o Titular ou um Terceiro tem um direito a ser exercido. Ela é especialmente utilizada no contexto de um contrato ou processo judicial – como no caso da necessidade de tratar Dados Sensíveis para apurar denúncias de má-conduta no GRUPO SOMA.</p>
<p>Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária <i>(Exclusiva para casos de tratamento de Dados Sensíveis)</i></p>	<p>É a Base Legal aplicável ao tratamento de Dados Sensíveis de saúde quando a atividade objetiva tutelar a saúde do Titular. É o caso de parte dos procedimentos realizados em clínicas, hospitais e seguradoras de saúde.</p> <p>Essa Base Legal exige que o Tratamento seja realizado por profissionais da saúde, serviços de saúde ou autoridade sanitária.</p>

<p>Garantia da prevenção à fraude e à segurança do Titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos</p> <p><i>(Exclusiva para casos de tratamento de Dados Sensíveis)</i></p>	<p>É a hipótese que autoriza o uso de Dados Sensíveis – notadamente biometria – para processos de identificação e autenticação do Titular. É o caso, por exemplo, do registro de ponto biométrico ou do duplo fator de autenticação em algumas aplicações bancárias.</p> <p>Essa Base Legal não pode ser utilizada quando prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos Dados Pessoais.</p>
---	--

7. REGISTRO DE TRATAMENTO

A LGPD estabelece a obrigação de manter um registro de atividades de Tratamento de Dados Pessoais. Todos os novos tratamentos de dados devem ser informados ao Escritório de Privacidade, que analisará este novo Tratamento, o incluirá no Registro de Atividades de Tratamento de Dados Pessoais e, caso necessário, apontará adequações.

Entre as possíveis recomendações, sem limitação, poderá haver a necessidade de (i) elaboração e aprovação de um Teste de Legítimo Interesse ou de um Relatório de Impacto à Proteção de Dados; (ii) contratação ou implementação de ferramenta para coleta e gestão de consentimento, se necessário; e (iii) limitação de acesso aos dados ou alterações no procedimento inicialmente previsto como forma de atender aos requisitos da legislação.

8. PRIVACY BY DESIGN E RELATÓRIO DE IMPACTO

Todo e qualquer projeto do GRUPO SOMA, particularmente relacionado ao desenvolvimento de novos produtos, software e serviços, que envolva o Tratamento de Dados Pessoais, deverá observar os princípios da LGPD e as disposições da legislação aplicável, com ênfase na preservação da privacidade dos Titulares e na proteção dos Dados Pessoais.

Para isso, é importante que todos os Colaboradores tenham um bom entendimento das obrigações de proteção de dados (conforme estabelecido nesta Política), garantindo que o conceito de proteção de dados seja observado desde a concepção do produto ou do serviço até a sua execução. Para tanto, serão conduzidos treinamentos para que os Colaboradores se familiarizem com os conceitos e obrigações desta Política e da legislação, bem como deverá ser preenchido um Questionário de *Privacy by Design* pelo Colaborador.

Caso o novo produto ou serviço envolva atividades de Tratamento de Dados Pessoais que possam gerar riscos aos Titulares, o Colaborador deverá solicitar o apoio do Encarregado para que seja realizada uma avaliação aprofundada dos impactos e riscos à privacidade e à proteção de Dados Pessoais. As avaliações poderão ser feitas por meio de Relatórios de Impacto à Proteção de Dados Pessoais, a fim de que sejam identificados os riscos e eventuais medidas, salvaguardas e mecanismos de mitigação.

9. TREINAMENTOS

O GRUPO SOMA está comprometido com a conscientização e disseminação das iniciativas de privacidade e proteção de dados por toda o GRUPO SOMA. Por isso, conta com planos contínuos e periódicos de treinamento dos Colaboradores sobre o tema.

É obrigação dos Colaboradores participar das atividades de treinamento do GRUPO SOMA e incorporar a privacidade e a proteção de dados pessoais nas suas atividades de trabalho, bem como consultar e observar todos dos documentos do GRUPO SOMA sobre o tema. Caso algum Colaborador tenha dúvidas ou queira aprofundar seu conhecimento sobre a proteção dos dados pessoais, pode encaminhar suas dúvidas e sugestões para o e-mail indicado ao final da Política.

10. COMPARTILHAMENTO DE DADOS E CONTRATAÇÕES

Para fins da presente Política, considera-se compartilhamento de Dados Pessoais toda e qualquer comunicação, difusão, transferência, interconexão de Dados Pessoais ou Tratamento compartilhado de bancos de Dados Pessoais, com órgãos, entidades ou organizações, públicas ou privadas. O Colaborador deverá garantir que os Dados Pessoais não sejam compartilhados com órgãos, entidades ou organizações (incluindo empresas parceiras ou prestadores de serviço), a menos que tenham sido firmados

acordos contratuais apropriados ou que a divulgação seja permitida pela legislação aplicável.

Os Colaboradores responsáveis por criar ou gerenciar relacionamentos com terceiros em nome do GRUPO SOMA devem obter garantias por escrito de que o terceiro tem a capacidade de proteger os Dados Pessoais, de acordo com os princípios contidos nesta Política. Isso pode ser feito por meio de *due diligence* de terceiros – seguindo as regras constantes na Política de Contratação de Fornecedores, avaliações de risco e contrato formal por escrito contendo cláusula-padrão – como os Modelos de Cláusula de Proteção de Dados do GRUPO SOMA, a critério do GRUPO SOMA.

Em caso de dúvidas, o Colaborador pode submeter a matéria para o canal de contato indicado ao final da Política.

11. TRANSFERÊNCIA INTERNACIONAL

A LGPD prevê critérios específicos para que a transferência internacional de dados seja permitida. Para garantir que o GRUPO SOMA esteja em conformidade, qualquer transferência internacional de Dados Pessoais – inclusive aquelas para fins de armazenamento em servidores de terceiros localizados fora do País – deverá ser comunicada ao Encarregado e ao Comitê de Privacidade previamente. A comunicação deverá se dar com antecedência à efetivação da transferência e deverão ser informados:

- a) País destinatário dos Dados Pessoais;
- b) Entidade que receberá os Dados Pessoais;
- c) Quais Dados Pessoais serão transferidos e a categoria dos Titulares envolvidos (dados de Colaboradores, clientes ou fornecedores, por exemplo);
- d) Finalidade da transferência;
- e) Base Legal que embasa o Tratamento; e
- f) Como os Dados Pessoais em questão foram coletados pelo GRUPO SOMA.

Com base nessas informações, o Comitê de Privacidade e o Encarregado, em conjunto com o departamento Jurídico, averiguarão se a transferência atende aos critérios estabelecidos na LGPD e informarão os termos em que a transferência poderá ocorrer.

12. DIREITOS DOS TITULARES

A LGPD garante aos Titulares uma série de direitos exercíveis perante os Controladores. Dessa forma, todo aviso de privacidade ou outras comunicações feitas aos Titulares devem indicar a forma e o procedimento segundo o qual os Titulares poderão exercer os seus direitos previstos em lei. O Aviso de Privacidade do GRUPO SOMA, disponibilizado no seu website, apresenta uma seção específica (seção 3) com informações sobre cada um dos direitos previstos na LGPD e como o titular pode exercê-los.

Caso qualquer Colaborador receba qualquer pedido de um Titular relacionado à temática de privacidade e proteção de dados, o pedido em questão deverá ser direcionado imediatamente ao e-mail privacidade@somagrupo.com.br pelo Colaborador. Em determinados casos, a LGPD estabelece prazos específicos para o atendimento das solicitações dos Titulares. Sendo assim, o Colaborador que demorar a direcionar a demanda sem justificativa razoável cometerá infração a esta Política.

13. ENCERRAMENTO DO TRATAMENTO DE DADOS PESSOAIS

A retenção de Dados Pessoais é permitida quando há uma Base Legal válida e adequada para determinada finalidade legítima de Tratamento, inclusive quando os Dados Pessoais forem necessários para o cumprimento de obrigação legal ou regulatória pelo GRUPO SOMA. Em atendimento à legislação e ao princípio da necessidade, ao término da finalidade de Tratamento de Dados Pessoais, os Colaboradores devem seguir as determinações internas do GRUPO SOMA referentes à retenção e descarte dos Dados Pessoais, constantes na Procedimento de Retenção e Descarte de Dados.

14. RESPONSABILIDADES

Para manter o nível de adequação do GRUPO SOMA, todos os colaboradores terão responsabilidades específicas, conforme descrito abaixo e em documentos específicos que poderão ser criados e anexados à Política posteriormente.

14.1. Colaboradores em geral

- Ler, compreender e cumprir integralmente os termos desta Política de Governança em Privacidade e Proteção de Dados Pessoais e demais Políticas e Regulamentações implementadas pelo GRUPO SOMA.

- Tratar os Dados Pessoais sob sua responsabilidade somente para os fins autorizados por esta Política, de forma ética e legal, respeitando os direitos dos Titulares e a legislação aplicável;
- Zelar pela integridade, disponibilidade, confidencialidade e autenticidade dos Dados Pessoais Tratados, não os utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na internet, nos termos da Política de Segurança da Informação;
- Quando solicitado pelo Encarregado, aplicar as alterações indicadas para adequação das atividades de Tratamento de Dados Pessoais;
- Relatar imediatamente a ocorrência de quaisquer Incidentes ou suspeitas de Incidentes envolvendo Dados Pessoais, bem como as deficiências relacionadas a possíveis riscos, de acordo com a Plano de Resposta a Incidentes envolvendo Dados Pessoais;
- Comunicar, tempestivamente, mudanças substanciais ou nova atividade de tratamento de dados pessoais ao Escritório de Privacidade.
- Participar das atividades de treinamento em proteção de dados, conforme orientado.
- Responder pela inobservância das Políticas e procedimentos relacionados ao tratamento de dados pessoais, conforme definido no item sanções.

14.2. Comitê de Privacidade

- Aprovar e decidir sobre a substituição dos membros do Sub Comitê.
- Acompanhar os temas críticos de Privacidade e Proteção de Dados.
- Decidir sobre riscos extremo e alto, temas urgentes, ou que necessitem de validação.
- Disponibilizar os recursos necessários para uma efetiva Gestão da Privacidade e Proteção de Dados Pessoais.
- Solicitar ao encarregado de dados um reporte de incidentes e situações relacionadas a privacidade de dados no GRUPO SOMA.

14.3. Sub Comitê de Privacidade

- Propor, revisar e atualizar as diretrizes de Privacidade, a fim de garantir que as Políticas, as Normas e os Procedimentos de Privacidade e Proteção de Dados existentes estejam adequados às necessidades de negócio do GRUPO SOMA.
- Elaborar e gerenciar o plano estratégico e o orçamento para uma efetiva Gestão de Privacidade e de Proteção de Dados Pessoais.
- Avaliar a matriz de riscos relacionados à Privacidade elaborada pelas áreas competentes e garantir que sejam, preventivamente, tratados.
- Garantir que o tratamento de Dados Pessoais seja realizado em conformidade com as Políticas e com as Normas internas relacionadas à Privacidade, Proteção de Dados e à legislação vigente.
- Formalizar o aceite do risco residual relacionado à Privacidade e Proteção de Dados.
- Decidir sobre riscos médio e baixo e reportar os riscos extremo e alto para deliberação do Comitê de Privacidade.
- Aprovar as medidas técnicas e administrativas para proteger os Dados Pessoais e as medidas de continuidade com o objetivo de evitar a interrupção das atividades do negócio.
- Propor medidas de conformidade a fim de atender às regulamentações e às legislações nos locais onde o GRUPO SOMA atua e garantir que tais requisitos sejam inseridos nos contratos de prestação de serviços e nos contratos com seus fornecedores.
- Monitorar a implantação das ações do Programa de Privacidade.
- Garantir ações adequadas para treinamento e para conscientização sobre Privacidade e Proteção de Dados para colaboradores, fornecedores, franqueados, parceiros e prestadores de serviço.
- Ser agente multiplicador dos temas relacionados à Política de Privacidade e à Norma de Proteção de Dados.

14.4. Escritório de Privacidade / Encarregado (DPO)

- Aceitar reclamações e comunicações dos titulares de dados pessoais externos, prestar esclarecimentos e adotar as providências necessárias.
- Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar as providências necessárias.
- Atender as demais atribuições, conforme orientação da Autoridade Nacional de Proteção de Dados, definidas em normativas complementares publicadas pelo referido Órgão.
- Supervisionar o processo de divulgação de informações sobre privacidade e proteção de dados pessoais, bem como a entrega de relatórios à Autoridade Nacional de Proteção de Dados (ANPD).
- Manter o relacionamento com todas as áreas do GRUPO SOMA.
- Aplicar treinamentos e orientar os colaboradores, terceiros contratados e demais partes do GRUPO SOMA a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.
- Apoiar o Comitê de Privacidade em suas deliberações.
- Reportar atividades, resultados, indicadores e decisões acerca do Programa de Privacidade ao Comitê de Privacidade do GRUPO SOMA.
- Identificar e avaliar as principais ameaças à proteção de dados, bem como propor e, quando aprovado, apoiar a implantação de medidas corretivas para reduzir o risco.
- Atuar junto ao time de Segurança da Informação no ajuste das normativas e procedimentos de segurança da informação, necessários para se fazer cumprir a Política de Proteção de Dados Pessoais.
- Sugerir adequação em tecnologia, processos e treinamentos aos colaboradores do GRUPO SOMA.
- Tomar as ações cabíveis para se fazer cumprir a Governança em Privacidade e Proteção de Dados.

- Apoiar a gestão das violações de Dados Pessoais, garantindo tratamento adequado e comunicando, em prazo razoável, a Autoridade Nacional e Titulares afetados pela violação sempre que esta representar risco ou dano relevante aos Titulares.
- Coordenar a execução de Relatório de Impacto à Proteção de Dados Pessoais e Testes de Legítimo Interesse, quando necessário;
- Elaborar, revisar e atualizar as políticas relacionadas à privacidade e à proteção de dados;
- Manter o Registro de Atividades de Tratamento de Dados Pessoais devidamente atualizado;
- Avaliar o risco de terceiros envolvidos em atividades de Tratamento de Dados Pessoais, mantendo documentação apropriada.
- Revisar e avaliar o preenchimento de questionários *Privacy by Design*.

14.5. Gestores das áreas

- Responsabilizar-se pelo uso adequado de Dados Pessoais nas atividades de suas respectivas áreas;
- Assegurar que os Colaboradores sob sua supervisão sejam devidamente informados e compreendam os termos da presente Política e das políticas relacionadas;
- Garantir que as alterações sugeridas pelo Encarregado sejam devidamente avaliadas e respondidas;
- Informar o Encarregado sobre novas atividades de Tratamento de Dados Pessoais, de forma a manter o Registro de Atividades de Tratamento de Dados Pessoais atualizado;
- Realizar a gestão do ciclo de vida dos Dados Pessoais Tratados do seu departamento, conforme o que lhe seja aplicável da Política de Retenção e Descarte de Dados Pessoais.

14.6. Jurídico

- Assegurar que os contratos que contemplem Tratamento de Dados Pessoais contenham cláusulas de proteção de Dados Pessoais adequadas à legislação e regulamentação aplicáveis;
- Prestar apoio jurídico na ocorrência de vazamentos de dados pessoais e nos procedimentos de investigações de incidentes; ;
- Prestar apoio jurídico na interpretação da legislação e regulamentação relativas à proteção de Dados Pessoais;
- Prestar apoio jurídico na elaboração de respostas a requisições de Titulares ou de autoridades;
- Indicar a Base Legal adequada para as atividades de Tratamento de Dados Pessoais realizadas pelo GRUPO SOMA.

14.7. Segurança da Informação

- Analisar Incidentes envolvendo Dados Pessoais bem como efetuar a coleta de evidências técnicas nestes casos;
- Monitorar e implementar medidas de segurança para garantir o cumprimento da legislação e da regulamentação aplicáveis;
- Revisar e manter atualizadas as Políticas relativas à Segurança da Informação;
- Definir, em conjunto com o Encarregado, procedimento e *templates* para documentação de Incidentes envolvendo Dados Pessoais;
- Implementar mecanismos técnicos para garantir o atendimento aos direitos dos Titulares;
- Prestar suporte técnico e analisar novas ferramentas e sistemas com foco na proteção de Dados Pessoais;
- Gerenciar e auxiliar o Encarregado no cumprimento do Plano de Resposta a Incidentes;
- Garantir a aplicação das medidas de segurança proporcionais ao risco gerado pelo Tratamento de Dados Pessoais e em linha com a expectativa de proteção do Titular do Dado Pessoal, preservando a integridade, disponibilidade e confidencialidade destas informações;
- Definir os privilégios de acesso a sistemas, em conjunto com os respectivos departamentos, bem como auxiliar nas revisões periódicas destes.

15. SANÇÕES

Caso o Colaborador não cumpra as regras desta Política, ele estará sujeito à aplicação de sanções que serão recomendadas pelo Comitê de Privacidade ou pelo Encarregado de Proteção de Dados e aplicadas pela área de Gente e Gestão de acordo com o grau de gravidade da conduta praticada pelo Colaborador, podendo variar entre:

- (i) **advertência:** no caso de infrações consideradas leves;
- (ii) **suspensão:** no caso de infrações consideradas graves ou na hipótese de reincidência de uma conduta classificada leve; ou
- (iii) **encerramento do contrato:** no caso de infrações consideradas gravíssimas ou na hipótese de reincidência de conduta grave. Tratando-se de Colaborador empregado, isso pode significar o desligamento do Colaborador e a rescisão de seu contrato de trabalho por justa causa. Tratando-se de Colaborador não empregado, poderá ensejar a rescisão motivada do contrato, conforme aplicável.

Os Colaboradores que cometerem infração a esta Política serão comunicados por escrito, com cópia para o gestor responsável. Tal comunicação conterá a regra violada, a conduta praticada pelo Colaborador e a sanção aplicada pelo GRUPO SOMA, sem prejuízo de eventual indenização paga pelo Colaborador a ser apurada judicialmente.

16. ATUALIZAÇÃO DESTA POLÍTICA

Essa Política poderá ser revista, atualizada e alterada a qualquer tempo, a exclusivo critério do GRUPO SOMA sempre que algum fato relevante ou evento motive sua revisão antecipada. Em caso de dúvidas, comentários ou sugestões relacionadas a esta Política, favor entrar em contato pelo seguinte canal: privacidade@somagrupo.com.br