POLÍTICA DE PROTEÇÃO DE DADOS PARA CONTRATAÇÃO DE FORNECEDORES

A Política de Proteção de Dados para Contratação de Fornecedores ("Política") tem por finalidade orientar os colaboradores da **HOPE DO NORDESTE LTDA.** (o "**Grupo HOPE**" ou a "Empresa") sobre como proceder com a contratação de fornecedores quando envolver o tratamento de dados pessoais, visando minimizar riscos.

TODOS OS COLABORADORES DEVEM OBRIGATORIAMENTE CUMPRIR AS DISPOSIÇÕES EXPRESSAS NESTA POLÍTICA, INDEPENDENTEMENTE DE SEU CARGO, FUNÇÃO, ÁREA DE ATUAÇÃO. O NÃO CUMPRIMENTO DAS DISPOSIÇÕES ORA PREVISTAS SUJEITARÁ O COLABORADOR INFRATOR A SANÇÕES.

ÍNDICE

1. OBJETIVO

Esta Política visa orientar os Colaboradores do **Grupo HOPE** sobre os procedimentos relacionados à contratação de fornecedores, prestadores de serviços e parceiros de negócios (em conjunto denominados "Fornecedores") que envolva o tratamento de toda e qualquer informação relacionada a pessoa natural identificada ou identificável ("Dados Pessoais").

A Lei nº 13.709/18 (LGPD), a Lei nº 12.965/14 (Marco Civil da Internet – MCI) e demais regulações sobre o tema (em conjunto, "Legislação Aplicável") estabelecem parâmetros para a devida proteção dos Dados Pessoais.

Ao contratar Fornecedores que realizam o tratamento de Dados Pessoais no contexto da sua operação, o **Grupo HOPE** assume responsabilidade sobre toda a cadeia de tratamento dos Dados Pessoais, devendo, portanto, estabelecer procedimentos internos capazes de conferir o nível de adequação de tais Fornecedores à Legislação Aplicável. As orientações previstas nesta Política têm como principais objetivos:

(i) estabelecer procedimentos internos para a contratação de Fornecedores que envolva o tratamento de Dados Pessoais; e

(ii) assegurar que os Fornecedores tenham nível adequado de proteção dos Dados Pessoais, conforme a Legislação Aplicável.

2. APLICAÇÃO

A presente Política deve ser observada por todas as áreas do **Grupo HOPE**, inclusive por todas as pessoas físicas e jurídicas, sejam sócios, diretores, administradores, empregados, prestadores de serviços, parceiros ou quaisquer outros terceiros ("Colaboradores") que, no âmbito dessa relação, possam vir a contratar ou estabelecer relações comerciais com os Fornecedores. Esta Política deverá ser observada em conjunto com as demais políticas do **Grupo HOPE**.

3. PROCEDIMENTOS PRÉVIOS À CONTRATAÇÃO DE FORNECEDORES

Antes da contratação de um Fornecedor, os Colaboradores deverão seguir determinados procedimentos para que o **Grupo HOPE** seja capaz de avaliar a presença dos requisitos de proteção de dados e segurança da informação, de acordo com as necessidades do **Grupo HOPE**. As principais etapas ao iniciar a contratação de um Fornecedor são:

- ETAPA 1: Classificação da Contratação;
- ETAPA 2: Envio do Questionário de Proteção de Dados
- ETAPA 3: Aprovação dos Departamentos Responsáveis; e
- ETAPA 4: Monitoramento Constante do Fornecedor.

Dependendo da contratação, nem todas as etapas podem ser necessárias ou algumas etapas podem ser combinadas. Em alguns casos, pode ser apropriado adotar medidas adicionais específicas à natureza dos Dados Pessoais envolvidos na contratação. Cada contratação e cada Fornecedor devem ser analisados caso a caso, realizando uma avaliação dos riscos e usando essa avaliação para decidir o curso apropriado da contratação.

ETAPA 1. Classificação da Contratação.

Para os fins da presente Política, deve ser considerado tratamento de Dados Pessoais toda e qualquer 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.

As contratações devem ser classificadas conforme o nível de tratamento dos Dados Pessoais, de acordo com os seguintes tipos:

(i) **Fornecedor de baixa criticidade:** Trata-se de contratação na qual o Tratamento de Dados Pessoais não é central para a relação com o Fornecedor. Existem situações típicas no **Grupo HOPE** em que a contratação e relacionamento com o Fornecedor estaria dentro dessa classificação, como, por exemplo, as contratações que envolvam fornecimento de matéria prima para desenvolvimento dos produtos, materiais de escritório, serviços de limpeza, entre outros.

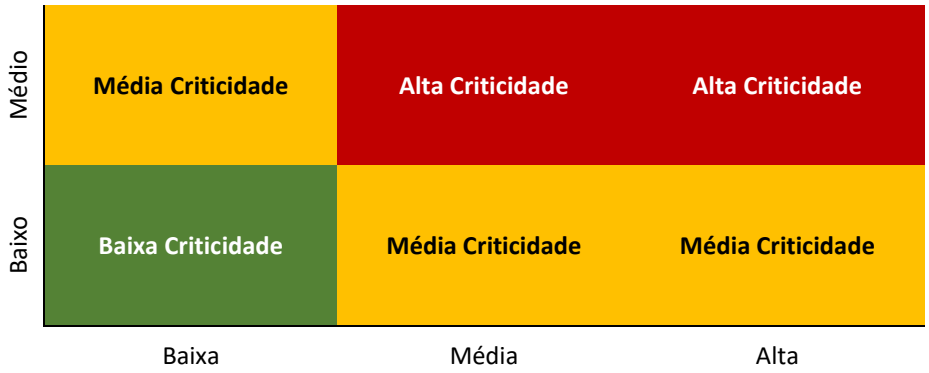
(ii) **Fornecedor de média criticidade:** Trata-se de contratação na qual o Tratamento de Dados Pessoais não é central para a relação com o Fornecedor, mas é necessário para que a relação se desenvolva. Existem situações no **Grupo HOPE** em que a contratação e relacionamento com o Fornecedor estaria dentro dessa classificação, por exemplo, as contratações relacionadas ao cumprimento de obrigações fiscais e contábeis, à realização de eventos e treinamentos para grupos de Colaboradores, entre outros.

(iii) **Fornecedor de alta criticidade:** Trata-se de contratação na qual o Tratamento de Dados Pessoais é central para a relação com o Fornecedor, sendo esse o objeto da relação desse Fornecedor com o **Grupo HOPE**. Existem situações no **Grupo HOPE** em que a contratação e relacionamento com o Fornecedor estaria dentro dessa classificação, por exemplo, as contratações relacionadas a ferramentas tecnológicas *SaaS*, benefícios a empregados e, no geral, quaisquer situações em que um Fornecedor se torne responsável pelo Tratamento de Dados Pessoais de clientes ou colaboradores do **Grupo HOPE**.

Além dos critérios gerais dispostos acima para a definição do nível de criticidade da relação com cada potencial Fornecedor, os seguintes elementos também devem ser levados em conta para o processo de classificação do Fornecedor:

- **Volume** de Dados Pessoais a que o Fornecedor tem ou pode vir a ter acesso; e
- **Sensibilidade** dos Dados Pessoais a que o Fornecedor tem ou pode vir a ter acesso.

Tais critérios devem ser aferidos utilizando as seguintes métricas:



VOLUME DE DADOS PESSOAIS TRATADOS	
Criticidade	**Descrição**
Alto	volume de Dados Pessoais tratado superior a 10% da base de dados controlada pela Empresa.
Médio	volume de Dados Pessoais tratado inferior a 10% e superior a 2% da base de dados controlada pela Empresa.
Baixo	volume de Dados Pessoais tratado inferior a 2% da base de dados controlada pela Empresa.

SENSIBILIDADE DOS DADOS PESSOAIS TRATADOS	
Criticidade	**Descrição**
Alta	Dados Pessoais de crianças ou adolescentes, Dados Pessoais Sensíveis ou que possam gerar discriminação aos titulares; dados bancários, de pagamento ou de proteção ao crédito.
Média	Dados Pessoais imediatamente identificáveis (e.g. nome, e-mail, CPF), combinados ou não com informações comportamentais (e.g. histórico de compras, preferências etc.)
Baixa	Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido compartilhada), Dados Pessoais de difícil identificação (e.g. IP).

ETAPA 2. Questionário de Proteção de Dados, Questionário de Conformidade e Aviso de Privacidade.

Caso a contratação envolva o tratamento de Dados Pessoais e a criticidade da contratação for média ou alta, o Colaborador deverá, antes de avançar em qualquer negociação, enviar o Questionário de Proteção de Dados, conforme modelo do Anexo I da presente Política.

ETAPA 3. Aprovação dos Departamentos Responsáveis.

Assim que o Questionário de Proteção de Dados do Anexo I for respondido pelo Fornecedor, este deverá ser encaminhado ao Departamento Jurídico e ao time de Segurança da Informação ("Departamentos Responsáveis"), por meio do seguinte endereço de e-mail privacidade@hopelingerie.com.br, para que avaliem o nível de conformidade do Fornecedor com as Legislação Aplicável de acordo com os critérios definidos no item 5 desta Política.

Caso os Departamentos Responsáveis entendam que as respostas do Fornecedor são suficientes, o Fornecedor será aprovado e o Colaborador poderá dar continuidade nas negociações. Caso contrário, os Departamentos Responsáveis poderão solicitar informações ou esclarecimentos adicionais e, se for o caso, sugerir a suspensão do processo de contratação.

Caso as condições contratuais sejam alteradas, sobretudo no que diz respeito ao tratamento de Dados Pessoais, esta etapa deverá ser reiniciada. Toda e qualquer contratação que envolva Dados Pessoais somente poderá ocorrer mediante aprovação prévia e expressa dos Departamentos Responsáveis.

ETAPA 4. Monitoramento Constante do Fornecedor.

Esta etapa será conduzida pelo time de tecnologia e segurança da informação do **Grupo HOPE**. Com o intuito de garantir a conformidade contínua com os requisitos de segurança da informação e de proteção de dados pessoais do **Grupo HOPE**, deverá ser realizado um monitoramento constante das atividades do Fornecedor, além de eventuais reavaliações periódicas sobre os critérios indicados no questionário preenchido pelo Fornecedor, especialmente com relação aos Fornecedores mais estratégicos e de criticidade alta.

4. AVALIAÇÃO DOS REQUISITOS DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO

Quando o Questionário de Proteção de Dados respondido pelo Fornecedor for recebido pelos Departamentos Responsáveis, estes deverão avaliar o nível de conformidade do Fornecedor com as Legislação Aplicável de acordo com os critérios definidos abaixo, levando-se em consideração todos os riscos técnicos e jurídicos inerentes às atividades de tratamento dos Dados Pessoais envolvidas no escopo da contratação correspondente.

Os Departamentos Responsáveis, após a devida avaliação, poderão estabelecer critérios essenciais na negociação das cláusulas de proteção de dados e segurança da informação para reger a relação jurídica entre as partes.

5.1. Padrões e Requisitos de Segurança

Para a devida avaliação dos padrões e requisitos de segurança do Fornecedor, o Departamento de Segurança da Informação deverá levar em consideração os seguintes critérios:

- Os Fornecedores devem manter documentadas políticas de segurança da informação apropriadas para mitigar riscos relacionados a incidente de segurança envolvendo Dados Pessoais;

- Os Fornecedores devem garantir que os Dados Pessoais envolvidos na contratação sejam protegidos adequadamente, adotando as melhores práticas de mercado considerando a criticidade dos Dados Pessoais.

5.2. Padrões e Requisitos de Proteção de Dados

Para a devida avaliação dos padrões e requisitos de proteção de Dados Pessoais, os Departamentos Responsáveis deverão levar em consideração os seguintes critérios:

a) Objeto da contratação

- O objeto da contratação deverá seguir todos os princípios da LGPD, sobretudo no que se refere à necessidade, adequação e finalidade do tratamento dos Dados Pessoais;

- Os Fornecedores deverão firmar com o **Grupo HOPE** contratos com cláusulas específicas de proteção de dados e adequadas ao tratamento dos Dados Pessoais e à operação, que será realizada conforme orientação do Departamento Jurídico.

b) Resposta a Notificação de Incidentes

- Os Fornecedores devem manter um plano de gerenciamento de incidentes que envolvam Dados Pessoais, devendo notificar o **Grupo HOPE**, em prazo razoável, toda e qualquer violação que, de forma acidental ou ilícita, enseje a destruição, perda, uso, alteração, divulgação ou acesso não autorizados aos Dados Pessoais ou qualquer forma de tratamento inadequado, ilícito ou indevido dos Dados Pessoais.

- Os Fornecedores devem ser capazes de identificar a causa dos incidentes e tomar as medidas apropriadas para remediar a causa do incidente, bem como estabelecer procedimentos para a continuidade dos negócios.

c) Medidas de Conscientização e Treinamento

- Os Fornecedores devem garantir que seus colaboradores recebam treinamentos e workshops de conscientização regulares e sejam informados dos requisitos de segurança aplicáveis.

5. DISPOSIÇÕES FINAIS

As exceções às regras estabelecidas por esta Política para atender alguma demanda específica devem ser apresentadas aos Departamentos Responsáveis para prévia avaliação e aprovação por escrito.

Essa Política poderá ser revista, atualizada e alterada anualmente ou a qualquer tempo, a exclusivo critério do **Grupo HOPE**, sempre que algum fato relevante ou evento motive sua revisão.

Quaisquer dúvidas em relação a este documento poderão ser encaminhadas ao e-mail privacidade@hopelingerie.com.br.

ANEXO I – QUESTIONÁRIO DE PROTEÇÃO DE DADOS

QUESTIONÁRIO PARA FORNECEDORES E PARCEIROS DO GRUPO HOPE

O **Grupo HOPE** preza pela privacidade de seus clientes, colaboradores e parceiros e trabalha para garantir a proteção dos dados pessoais em todas as suas atividades. Para isso, precisamos assegurar que nossos parceiros e fornecedores também se preocupam com a segurança e o uso adequado dos dados pessoais.

O **Grupo HOPE** elaborou este questionário para obter, junto aos futuros e atuais fornecedores e parceiros, informações e documentos que servirão para entender o nível de adoção de padrões de segurança da informação e de conformidade de cada fornecedor com a legislação de privacidade e proteção de dados no Brasil.

INSTRUÇÕES: Solicitamos, por gentileza, que você:

- responda às solicitações deste Questionário da forma mais completa e precisa possível;
- evite o uso de expressões como "etc.", "entre outros", bem como siglas que não são de conhecimento público;
- forneça, sempre que possível, comentários e esclarecimentos que sirvam para detalhar as informações solicitadas, tendo em mente que as pessoas que receberão as informações que você fornecer podem não conhecer as rotinas e as terminologias da sua empresa; e
- forneça, sempre que possível, documentos que possam servir para comprovar ou ilustrar melhor alguma informação fornecida, nos enviando os arquivos.

Caso não seja possível apresentar alguma informação ou documento específico, solicitamos que uma afirmação nesse sentido seja indicada e justificada nos comentários.

O **Grupo HOPE** agradece sua colaboração.

PARTE 1 - PERGUNTAS GERAIS

1. Favor informar o nome da empresa respondente (a "Empresa") e o CNPJ:

Empresa: Clique ou toque aqui para inserir o texto.	CNPJ: Clique ou toque aqui para inserir o texto.

2. Favor descrever a Empresa e suas atividades empresariais e, se houver, fornecer um link para seu *website*.

Resposta: Clique ou toque aqui para inserir o texto.

3. Onde a Empresa está sediada?

Resposta: Clique ou toque aqui para inserir o texto.

4. Quem é o colaborador da Empresa responsável pelo preenchimento deste Questionário? Favor fornecer informações de contato.

Incluindo nome, cargo, número de telefone e e-mail.

Resposta: Clique ou toque aqui para inserir o texto.

5. Quais atividades de tratamento de dados a Empresa realizará para o Grupo HOPE?

Ex.: fornecimento de plataforma de recrutamento, benefícios a colaboradores, atividades de marketing etc.

Resposta: Clique ou toque aqui para inserir o texto.

☐ Não tenho certeza
☐ Não aplicável

6. Quais produtos ou serviços a Empresa fornecerá ao Grupo HOPE? Favor descrever o produto ou serviço específico fornecido.

☐ Não aplicável

Resposta: Clique ou toque aqui para inserir o texto.

7. A Empresa utilizará algum suboperador/subcontratado para ajudá-la a entregar seus produtos ou serviços ao Grupo HOPE? Caso positivo, favor listar os suboperadores/subcontratados abaixo (e/ou incluir um link para o *website* deles) e enviar qualquer documentação relevante.

☐ Sim
☐ Não
☐ Não tenho certeza
☐ Não aplicável

Justifique sua resposta abaixo.

Resposta: Clique ou toque aqui para inserir o texto.

***8.* Onde serão hospedados os dados para esses produtos ou serviços?**

Ex.: Servidor localizado em São Paulo/SP | Servidor de terceiro (AWS) localizado nos EUA.

Resposta: Clique ou toque aqui para inserir o texto.

9. Se for o caso, qual empresa hospedará os dados para esses produtos ou serviços em nome da Empresa?

Resposta: Clique ou toque aqui para inserir o texto.

9.1. A Empresa tem documentos de suporte sobre o programa de privacidade/segurança da empresa que hospedará os dados disponível para revisão?

☐ Certificação ISO 27001
☐ Certificação BS 10012
☐ Relatório SOC 2
☐ Questionário SIG (*Standardized Information Gathering*)
☐ CSA SAIQ
☐ CSA STAR
☐ Código de Conduta aprovado sob a GDPR
☐ Informe de Privacidade/Segurança
☐ Política de Privacidade
☐ Política de Segurança da Informação

☐ Plano de Resposta a Incidentes
☐ Plano de Continuidade de Negócios
☐ Não aplicável
☐ Outro

Justifique sua resposta abaixo e forneça a documentação aplicável.

Resposta: Clique ou toque aqui para inserir o texto.

10. Haverá o compartilhamento de informações confidenciais (incluindo dados pessoais, sensíveis ou não) do Grupo HOPE com a Empresa?

☐ Sim
☐ Não
☐ Não tenho certeza

Justifique sua resposta abaixo.

Resposta: Clique ou toque aqui para inserir o texto.

11. Haverá o compartilhamento de qualquer tipo de dado pessoal com o Grupo HOPE? Em caso positivo, favor informar quais as categorias de titulares de dados que a Empresa tratará dados?

Ex.: Colaboradores, ex-funcionários, consumidores, parceiros comerciais etc.
☐ Sim
☐ Não
☐ Não tenho certeza

Resposta: Clique ou toque aqui para inserir o texto.

Justifique sua resposta abaixo.

Tipo de dado pessoal	Finalidade do tratamento	Base legal para o tratamento	Justificativa da base legal
Inserir texto	Inserir texto	Inserir texto	Inserir texto
Inserir texto	Inserir texto	Inserir texto	Inserir texto
Inserir texto	Inserir texto	Inserir texto	Inserir texto

12. Haverá tratamento de dados de crianças?

☐ Sim
☐ Não
☐ Não tenho certeza

Em caso positivo, forneça mais detalhes sobre o tratamento abaixo.

Resposta: Clique ou toque aqui para inserir o texto.

13. Haverá transferência internacional de qualquer tipo de dado pessoal?

Ex.: um fornecedor de tecnologia (ex: analytics, marketing, BI) que presta seus serviços fora do Brasil.
☐ Sim

☐ Não
☐ Não tenho certeza

Em caso positivo, favor informar os países em que os dados poderão ser transferidos:

Resposta: Clique ou toque aqui para inserir o texto.

PARTE 2 | ANÁLISE DE PRIVACIDADE DO FORNECEDOR

1. Algum dos dados pessoais que serão compartilhados com o Grupo HOPE estão publicamente disponíveis?

☐ Sim
☐ Não
☐ Não tenho certeza
☐ Não aplicável

Justifique sua resposta abaixo.

Resposta: Clique ou toque aqui para inserir o texto.

2. A Empresa dispõe de uma política de privacidade publicamente disponível?

☐ Sim
☐ Não

Favor fornecer um link para a política de privacidade, se houver.

Resposta: Clique ou toque aqui para inserir o texto.

3. A Política de Privacidade contém as seguintes características?

Selecione todas as afirmações aplicáveis:

☐ É concisa e transparente
☐ É inteligível
☐ É facilmente acessível
☐ Usa linguagem clara e simples
☐ É apresentada por escrito ou por outros meios
☐ É gratuita
☐ Dispõe sobre quais dados a Empresa coleta do usuário
☐ Dispõe a finalidade específica do tratamento dos dados
☐ Dispõe a forma e duração do tratamento e armazenamento
☐ Identifica o controlador
☐ Traz informações de contato do controlador
☐ Traz informações acerca do uso compartilhado de dados pelo controlador e a finalidade
☐ Informa as responsabilidades dos agentes que realização o tratamento
☐ Dispõe expressamente os direitos dos titulares de dados
☐ Informa como funciona a segurança da informação
☐ Não aplicável

Justifique sua resposta abaixo.

Resposta: Clique ou toque aqui para inserir o texto.

4. Como você classificaria o programa de privacidade geral da Empresa?

☐ Muito forte

☐ Forte
☐ Mediano
☐ Fraco
☐ Muito fraco

Favor explicar sua classificação abaixo.

Resposta: Clique ou toque aqui para inserir o texto.

PARTE 3 | ANÁLISE DE SEGURANÇA

1. Quais medidas técnicas a Empresa utiliza para proteção dos dados pessoais?

Selecione todas as afirmações aplicáveis:

☐ Lista de controle de acesso
☐ Anonimização de dados
☐ Anti-Malware
☐ Ferramentas de detecção de vazamentos
☐ Backup de dados
☐ Criptografia
☐ Firewalls
☐ Ferramentas de detecção de invasões
☐ Registro de dados (*data logging*)
☐ Controle de acesso lógico
☐ Ferramentas de gerenciamento de dispositivos móveis (*MDM Tools*)
☐ Autenticação multifatorial
☐ Autenticação de redes
☐ Pseudonimização de dados
☐ Atualizações regulares de software
☐ Ferramentas de detecção de vulnerabilidades
☐ Não aplicável

Caso a Empresa utilize de uma técnica não elencada acima, favor adicionar abaixo:

Resposta: Clique ou toque aqui para inserir o texto.

2. Quais medidas organizacionais para a proteção de dados a Empresa toma em relação aos produtos ou serviços que a Empresa fornecerá ao Grupo HOPE?

Selecione todas as afirmações aplicáveis:

☐ Políticas internas
☐ Revisões de acesso
☐ Conscientização e treinamento
☐ Acordos de processamento de dados
☐ Restrições de acesso a colaboradores específicos
☐ Políticas de senha
☐ Testes de penetração
☐ Plano de teste regular
☐ Descarte seguro

☐ Instalações seguras
☐ Controle segmentado de acesso
☐ Supervisão
☐ Não aplicável

Caso a Empresa utilize de uma técnica não elencada acima, favor adicionar abaixo:

Resposta: Clique ou toque aqui para inserir o texto.

3. Como você classificaria o programa de segurança geral da Empresa?

☐ Muito forte
☐ Forte
☐ Mediano
☐ Fraco
☐ Muito fraco

Favor explicar sua classificação abaixo.

Resposta: Clique ou toque aqui para inserir o texto.

PARTE 4 | INFORMAÇÕES ADICIONAIS

1. O Grupo HOPE agradece sua ajuda e disponibilidade para o preenchimento desse questionário! Caso tenha alguma informação adicional, favor inserir abaixo, anexando qualquer documento adicional, se houver.

Resposta: Clique ou toque aqui para inserir o texto.