

# Política de Proteção de Dados



PERFORMING DREAMS

## Índice

|   |    |
|---|----|
| <b>1. Âmbito e Objetivo</b>   | 4  |
| <b>2. Leis de proteção de dados</b>   | 5  |
| <b>3. Responsabilidade</b>  | 5  |
| <b>4. Definições</b>  | 5  |
| Unidade de negócio  | 6  |
| Consentimento   | 6  |
| Responsável pelo Processamento  | 6  |
| Titular dos dados   | 6  |
| EEE   | 6  |
| RGPD  | 6  |
| Responsáveis Conjuntos  | 6  |
| Dados pessoais  | 7  |
| Em processamento  | 7  |
| Violação de Dados Pessoais  | 7  |
| Processador   | 8  |
| Categorias especiais de dados (Dados Sensíveis)                             | 8  |
| País Terceiro   | 8  |
| <b>5. Diretrizes gerais da equipa</b>                                       | 8  |
| <b>6. Princípios-chave da Política de Proteção de Dados</b>                 | 9  |
| Direitos dos Titulares dos Dados  | 9  |
| Informação sobre os direitos dos Titulares dos Dados                        | 11 |
| <b>7. Armazenamento de dados</b>  | 11 |
| <b>8. Utilização de dados</b>   | 12 |
| <b>9. Precisão de dados</b>   | 13 |
| <b>10. Princípios gerais de privacidade observados pelo Grupo Visabeira</b> | 13 |
| Legalidade, justiça e transparência   | 14 |
| Limitação de finalidade   | 14 |
| Minimização de dados, precisão e limitação de armazenamento                 | 14 |
| Processamento Legal dos Dados Pessoais                                      | 14 |
| Processamento de Dados Sensíveis  | 15 |
| Condições para o consentimento  | 16 |
| Procedimento para lidar com as solicitações do Titular de Dados             | 17 |
| Confidencialidade do Processamento  | 17 |

---

|   |                                     |
|---|-------------------------------------|
| Responsáveis Conjuntos.....   | 17                                  |
| Utilização de processadores de dados .....  | 18                                  |
| Proteção de dados por desenho e por omissão.....  | 20                                  |
| Notificação de Violação de Dados Pessoais .....   | 20                                  |
| <b>11. Transferências.....</b>  | <b>21</b>                           |
| Transferência de Dados Pessoais para Responsáveis pelo Processamento e Processadores que são membros do grupo (transferência interna) ..... | 21                                  |
| Transferência entre Responsáveis pelo Processamento.....  | 21                                  |
| Transferência para Processadores fora do EEE .....  | 21                                  |
| <b>12. Alterações à Política Interna de Proteção de Dados.....</b>  | <b>22</b>                           |
| Documentos relacionados.....  | <b>Erro! Marcador não definido.</b> |

## 1. Âmbito e Objetivo

A presente Política Interna de Proteção de Dados (“**Política de Proteção de Dados**”) estabelece os princípios para o Tratamento de Dados Pessoais no Grupo Visabeira, S.A., doravante designado por “Grupo Visabeira”, e facilita o cumprimento das obrigações de proteção de dados do Grupo Visabeira.

Esta Política de Proteção de Dados aplica-se ao Grupo Visabeira e às suas subsidiárias e aplica-se a todos os colaboradores do Grupo Visabeira e ao Tratamento de Dados Pessoais no Grupo Visabeira. Esta Política será revista e atualizada periodicamente. O incumprimento desta Política de Proteção de Dados por parte dos colaboradores do Grupo Visabeira pode dar origem à aplicação de sanções disciplinares.

Esta Política de Proteção de Dados também se pode referir e deve ser lida em conjunto com as várias políticas do Grupo Visabeira relevantes para o Processamento de Dados Pessoais, incluindo, mas não se limitando a: Política de Segurança da informação, Notificação de Privacidade - Colaborador, Notificação de Privacidade para Parceiros de Negócios, Notificação de Privacidade - Clientes e Registos de Atividade de Processamento.

O Grupo Visabeira necessita de recolher e utilizar determinadas informações sobre indivíduos. Esses indivíduos podem incluir, por exemplo, os próprios colaboradores do Grupo Visabeira, os colaboradores dos nossos clientes e fornecedores, contratos comerciais e outros indivíduos com os quais a organização tenha algum tipo de relacionamento ou necessite de entrar em contacto. Esta Política de Proteção de Dados reflete e detalha o respeito do Grupo Visabeira pela privacidade desses indivíduos e o seu compromisso para com o cumprimento da legislação de proteção de dados aplicável.

Esta Política de Proteção de Dados estabelece um padrão básico de *compliance*. Nos casos em que as leis locais em vigor apliquem padrões mais rígidos, o Grupo Visabeira procurará seguir esses padrões. Sempre que aplicável, cada país deverá aderir a quaisquer requisitos adicionais ou desvios desta Política de Proteção de Dados, que sejam exigidos pelas leis locais aplicáveis.

Se pretender discutir o conteúdo desta Política de Proteção de Dados ou tiver alguma dúvida ou questão relativamente à privacidade ou proteção de dados no Grupo Visabeira, deverá contactar o *Data Protection Officer* (“DPO”) [Responsável pela Proteção de Dados] do Grupo Visabeira em [dpo@grupovisabeira.com](mailto:dpo@grupovisabeira.com).

## 2. Leis de proteção de dados

Existem várias leis de proteção de dados em todo o mundo que regulam a forma como o Grupo Visabeira utiliza Dados Pessoais.

Por exemplo, onde quer que o Grupo Visabeira esteja estabelecido no Espaço Económico Europeu ou no Reino Unido, deverá cumprir os requisitos do Regulamento Geral de Proteção de Dados da UE e do Regulamento Geral de Proteção de Dados do Reino Unido, respetivamente, bem como outras leis locais aplicáveis que apoiam o RGPD. Sempre que aplicável, o RGPD é sustentado por oito importantes princípios, que determinam que os Dados Pessoais devem:

- Ser processados de forma justa e legal;
- Ser obtidos apenas para fins específicos e legais;
- Ser adequados, relevantes e não excessivos;
- Ser precisos e atualizados;
- Não ser retidos por mais tempo do que o necessário;
- Ser processados de acordo com os direitos dos Titulares dos Dados;
- Ser protegidos de forma apropriada;
- Não ser transferidos para fora do Espaço Económico Europeu ("EEE"), a menos que esse país ou território também garanta um nível adequado de proteção.

## 3. Responsabilidade

Esta Política de Proteção de Dados está vinculada às Notificações de Segurança da Informação e Proteção de Dados do Grupo Visabeira, estando, como tal, sob responsabilidade do Departamento de TI. O Departamento de TI é responsável por garantir que a Política de Proteção de Dados seja aplicada em todas as Unidades de Negócio. A Organização de Proteção de Dados, através da Comissão de Segurança e Privacidade ("CSP") conforme descrito neste documento, é responsável pela implementação da Política de Proteção de Dados. Todos os colaboradores do Grupo Visabeira são responsáveis pelo cumprimento desta Política.

O Grupo Visabeira e cada Unidade de Negócio agindo como Responsável pelo Processamento, serão responsáveis pelo cumprimento desta Política de Proteção de Dados.

## 4. Definições

As seguintes definições devem ter o mesmo significado que as definições relevantes estabelecidas no RGPD.

**Unidade de negócio**

Unidade de Negócio significa todas as subsidiárias nas quais o Grupo Visabeira controla direta ou indiretamente mais de 50% do capital com direito a voto.

**Consentimento**

Consentimento significa qualquer indicação dada livremente, específica, informada e inequívoca da vontade de um Titular dos Dados pela qual o Titular dos Dados, por uma declaração ou uma ação afirmativa clara, manifesta o seu consentimento para o Tratamento dos Dados Pessoais que lhe digam respeito.

**Responsável pelo Processamento**

O Responsável pelo Processamento é uma pessoa física ou jurídica, por exemplo o Grupo Visabeira e/ou uma Unidade de Negócio, que isoladamente ou em conjunto com terceiros determina a finalidade e os meios de Tratamento de Dados Pessoais.

**Titular dos dados**

Uma pessoa singular identificada ou identificável, que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos associados a um dado físico ou fisiológico, à identidade genética, mental, económica, cultural ou social dessa pessoa física. Um Titular dos Dados pode ser, por exemplo, um colaborador ou contratante do Grupo Visabeira, um representante de um cliente ou fornecedor, uma pessoa que se candidate a um emprego no Grupo Visabeira ou subscreva informações inserindo informações no site do Grupo Visabeira ou um representante de um parceiro comercial do Grupo Visabeira.

**EEE**

O Espaço Económico Europeu, ou seja, os estados membros da UE, juntamente com os países da EFTA (Liechtenstein, Islândia e Noruega).

**RGPD**

O RGPD significa o Regulamento Geral de Proteção de Dados da UE 2016/679.

**Responsáveis Conjuntos**

Responsáveis Conjuntos significa a situação em que dois ou mais Responsáveis pelo Processamento determinam conjuntamente os propósitos e meios do Processamento.

### Dados pessoais

Dados Pessoais significa qualquer informação relacionada com um indivíduo identificado ou identificável (o “Titular dos Dados”). Os Dados Pessoais incluem todos os tipos de informações que, direta ou indiretamente, possam estar vinculados ao Titular dos Dados.

A título de exemplo, os Dados Pessoais podem incluir:

- Nomes, datas de nascimento, SAP ID, detalhes do passaporte;
- Detalhes de contacto, como moradas, endereços de e-mail, números de telefone, identificação de mensagens instantâneas e perfis de redes sociais;
- Informações indiretas, como endereço IP e nome do portátil;
- A expressão de opiniões sobre pessoas vivas;
- Dados de localização;
- Informações sobre salários e informações de pagamento;
- Informações de clientes e fornecedores (se vinculadas a um indivíduo).

### Em processamento

Qualquer operação ou conjunto de operações que seja realizada sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, através de meios automáticos ou não, como utilização, recolha, registo, organização, estruturação, alinhamento ou combinação, adaptação ou alternância, recuperação, consulta, disseminação, armazenamento e divulgação por transmissão ou disponibilização, restrição, apagamento ou destruição.

A definição é tecnologicamente neutra e inclui o Processamento de Dados Pessoais que é total ou parcialmente realizado com o auxílio de computadores ou equipamentos idênticos capazes de Processar Dados Pessoais automaticamente. A definição também inclui registos manuais ou sistemas de arquivo se os Dados Pessoais estiverem incluídos ou se destinarem a fazer parte de uma coleção estruturada, disponibilizando os Dados Pessoais para pesquisa ou compilação de acordo com critérios específicos.

### Violação de Dados Pessoais

Violação de Dados Pessoais significa uma violação de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a Dados Pessoais transmitidos, armazenados ou de outra forma processados, tais como:

- Informações indiretas, como endereço IP e nome do computador;
- A expressão de opiniões sobre pessoas vivas;
- Dados de localização;

- Informações sobre salários e informações de pagamento;
- Informações de clientes e fornecedores (se vinculadas a um indivíduo).

### Processador

Uma pessoa física ou jurídica, autoridade pública, agência ou outro órgão que processa os dados pessoais em nome de um Responsável pelo Processamento, por exemplo um parceiro de *outsourcing* ou um fornecedor de serviços que processa dados pessoais em nome de uma Unidade de Negócio.

### Categorias especiais de dados (Dados Sensíveis)

Categorias especiais de dados são Dados Pessoais que revelem ou digam respeito a:

- origem racial ou étnica;
- opiniões políticas;
- crenças religiosas ou filosóficas;
- filiação sindical;
- dados genéticos;
- dados biométricos com a finalidade de identificar exclusivamente um Titular dos Dados;
- saúde;
- vida sexual ou orientação sexual.

### País Terceiro

País Terceiro, no contexto de transferências internacionais, significa qualquer país fora do Espaço Económico Europeu ("EEE") que tenha sido considerado pela autoridade supervisora ou governamental relevante do país de exportação como não tendo leis de proteção de dados adequadas.

## 5. Diretrizes gerais da equipa

- A equipa só deve poder aceder aos Dados Pessoais abrangidos por esta Política de Proteção de Dados se for necessário para realizar o seu trabalho;
- Os dados não devem ser partilhados informalmente. Quando for necessário aceder a grandes volumes de Dados Pessoais ou Dados Pessoais inerentemente privados, os colaboradores podem solicitá-los aos seus superiores;
- O Grupo Visabeira dará formação a todos os colaboradores para os ajudar a compreender as suas responsabilidades no tratamento de dados pessoais, e disponibilizará uma plataforma de *e-learning*, para que possam aceder à informação sobre a disponibilização de novas formações e material de apoio relacionado;



- Os colaboradores devem manter todos os dados seguros, tomando precauções sensatas e seguindo as diretrizes abaixo indicadas;
- Em particular, devem ser utilizadas palavras-passe fortes, que nunca devem ser partilhadas;
- Os Dados Pessoais não devem ser divulgados a pessoas não autorizadas, quer seja dentro da empresa ou a nível externo;
- Os Dados Pessoais devem ser revistos periodicamente e devem atualizados quando se encontrarem desatualizados. Caso já não sejam necessários, deverão ser descartados.
- Os colaboradores deverão solicitar ajuda ao seu superior ou ao DPO se não tiverem certezas sobre qualquer aspeto relativo à proteção de dados.

## 6. Princípios-chave da Política de Proteção de Dados

### Direitos dos Titulares dos Dados

Os Titulares dos Dados (por exemplo, colaboradores, contratantes, clientes individuais e outros terceiros) cujos Dados Pessoais estejam a ser tratados por entidades do Grupo Visabeira sujeitas ao RGPD beneficiam dos seguintes direitos:

#### Informações sobre como seus Dados Pessoais estão a ser utilizados:

Os Titulares dos Dados têm o direito de ser informados sobre a forma como o Grupo Visabeira utilizará e partilhará os seus Dados Pessoais. Esta explicação deve ser facultada aos indivíduos de forma concisa, transparente, inteligível e de fácil acesso. As notificações de privacidade devem ser escritas em linguagem clara e simples e devem ser fornecidas de forma gratuita.

#### Direitos de acesso:

Ao abrigo do direito de acesso, os Titulares dos Dados têm o direito de:

- obter a confirmação de que o Grupo Visabeira está a Processar os seus Dados Pessoais;
- acesso aos seus Dados Pessoais; e
- informações sobre como os seus Dados Pessoais estão a ser utilizados pelo Grupo Visabeira.

Todos os pedidos dos titulares dos dados são tratados pelo DPO através de uma plataforma de CRM e respondidos dentro do prazo legal. Os pedidos de acesso e eliminação de dados são também tratados através de um caso de suporte, dirigido às entidades relevantes para o tratamento dos dados em causa.

Mais informações sobre o procedimento para lidar com solicitações de Titulares dos Dados

podem ser encontradas na secção 10 desta Política de Proteção de Dados.

**Direito de retificação:**

Os Titulares dos Dados têm o direito de retificar quaisquer Dados Pessoais inexatos ou incompletos.

**Direito de eliminação (em determinadas circunstâncias):**

Os Titulares dos Dados têm o direito de solicitar que determinadas informações detidas pelo Grupo Visabeira sejam apagadas. Tal também é conhecido como o direito de ser esquecido. Não se trata de um direito absoluto ou geral de exigir que todos os Dados Pessoais sejam excluídos. Por exemplo, se a informação for necessária para exercer ou defender ações judiciais, não é necessário que o Grupo Visabeira apague os Dados Pessoais.

**Direito de restringir o processamento e bloqueio de dados:**

Os Titulares dos Dados têm o direito de bloquear o processamento dos seus dados pessoais em determinadas circunstâncias. Se for feita uma solicitação para restringir o Processamento, será necessário que o Grupo Visabeira determine se a solicitação deve ser mantida e se é necessário implementar procedimentos para restringir a utilização dos Dados Pessoais relevantes.

**Direito à portabilidade de dados:**

Em determinadas circunstâncias, os Titulares dos Dados podem solicitar receber uma cópia dos seus Dados Pessoais num formato eletrónico comumente utilizado. Este direito aplica-se apenas às informações que os Titulares dos Dados tenham fornecido ao Grupo Visabeira (por exemplo, preenchendo um formulário ou fornecendo informações através de um site).

**Direito de se opor ao Processamento em determinadas circunstâncias (por exemplo, quando os Dados Pessoais são utilizados para fins de marketing):**

Os Titulares dos Dados têm o direito geral de se oporem ao processamento de dados realizado pelo Grupo Visabeira em determinadas circunstâncias (por exemplo, se o Grupo Visabeira estiver a utilizar dados pessoais para fins de marketing direto). Qualquer colaborador do Grupo Visabeira que receba uma objeção ao marketing deve garantir que o Titular dos Dados relevantes seja identificado no sistema, ou registo relevante, como tendo optado por não participar. Em caso de dúvida, entrar em contacto com o DPO do Grupo Visabeira.

### **Direitos em relação à tomada de decisão automatizada e criação de perfis:**

Os Titulares dos Dados têm o direito de não ficar sujeitos a uma decisão baseada num Processamento automático, onde a decisão produzirá um efeito legal, ou outro efeito igualmente significativo, sobre eles. Se for um colaborador do Grupo Visabeira e suspeitar que tal Processamento está a ser levado a cabo, deverá procurar orientação junto do DPO do Grupo Visabeira relativamente às medidas que precisam de ser tomadas para garantir que a decisão automatizada seja realizada de forma compatível com esta Política.

### **Informação sobre os direitos dos Titulares dos Dados**

Os Titulares dos Dados que beneficiem dos direitos previstos nesta Política de Proteção de Dados podem encontrar mais informações sobre o exercício dos seus direitos nas notificações de privacidade para: Clientes, Parceiros de negócios e Colaboradores.

## **7. Armazenamento de dados**

Essas regras descrevem como e onde os dados devem ser armazenados em segurança. As dúvidas sobre como armazenar dados com segurança podem ser direcionadas ao Departamento de TI ou ao Controlador.

### **Dados físicos (ou seja, documentos impressos)**

Quando os dados são armazenados em papel, eles devem ser mantidos num local seguro onde pessoal não autorizado não os possa ver. Especificamente:

- Quando não forem necessários, o suporte em papel ou os arquivos devem ser mantidos numa gaveta trancada ou num armário de arquivo;
- Os colaboradores devem certificar-se que o suporte em papel e as impressões não sejam deixados sem supervisão onde pessoal não autorizado possa vê-los, como uma mesa ou uma impressora;
- As impressões de dados devem ser destruídas e descartadas em segurança quando já não forem necessárias.

Informações adicionais sobre a segurança de dados físicos também podem ser encontradas na nossa Política de Segurança (ou seja, GVB Procedimento de Gestão de Acesso a Instalações Críticas) e na Política de *Backup* (GV Política de *Backup*).

### Dados eletrónicos

Quando os dados são armazenados em formato eletrónico, devem ser protegidos contra o acesso não autorizado, exclusão acidental e tentativas maliciosas de *hacking*. Devem ser tomadas as seguintes medidas para proteger os dados eletrónicos:

- Os dados devem ser protegidos por palavra-passes fortes que são alteradas a cada 90 dias (no mínimo) e não devem nunca ser partilhadas entre colaboradores;
- Se os dados estiverem armazenados em dispositivos amovíveis (como um CD ou um DVD), estes devem ser mantidos fechados em segurança quando não estiverem a ser utilizados;
- Os dados devem ser armazenados apenas em unidades e servidores designados para o efeito e só devem ser carregados para um sistema de *cloud* aprovado;
- Os servidores que contêm Dados Pessoais devem estar em local seguro, afastado do espaço geral do escritório;
- Deve-se fazer *backup* dos dados com frequência. Estes *backups* devem ser testados regularmente, de acordo com os procedimentos de *backup* padrão da empresa;
- Os dados nunca devem ser guardados diretamente em portáteis ou outros dispositivos móveis, como *tablets* ou *smartphones*;
- Todos os servidores e computadores que contêm dados devem ser protegidos por software de segurança aprovado e uma *firewall*;
- Todos os sistemas deverão ser atualizados de forma centralizada e periodicamente com os mais recentes antivírus e *firewalls*.

### **8. Utilização de dados**

Os Dados Pessoais não têm valor para o Grupo Visabeira, a menos que a empresa possa fazer uso deles. No entanto, é quando se acede e utiliza os Dados Pessoais que estes correm o maior risco de perda, corrupção ou roubo. Portanto:

- Ao trabalhar com Dados Pessoais, os colaboradores devem garantir que os ecrãs dos seus computadores estejam sempre bloqueados quando deixados sem vigilância;
- Os Dados Pessoais não devem ser partilhados informalmente. Em particular, grandes volumes de Dados Pessoais ou Dados Pessoais inerentemente privados (ou outros conjuntos de Dados Pessoais que tenham o potencial de criar riscos para indivíduos, se interceptados) nunca devem ser enviados por e-mail sem serem encriptados;

- Os dados devem ser encriptados antes de serem transferidos eletronicamente. O responsável de TI pode explicar como enviar dados para contactos externos autorizados;
- Os Dados Pessoais nunca devem ser transferidos para fora do Espaço Económico Europeu sem consulta prévia ao *Data Protection Officer* [Responsável pela Proteção de Dados];
- Os colaboradores não devem guardar cópias de Dados Pessoais nos seus próprios computadores. Em vez disso, os colaboradores devem sempre aceder e atualizar a cópia central de todos os dados.

### 9. Precisão de dados

A lei exige que o Grupo Visabeira, bem como os seus colaboradores, tomem as medidas necessárias para garantir que os dados sejam mantidos precisos e atualizados. Essas etapas devem incluir, mas não estão limitadas a:

- Sempre que possível, manter os Dados Pessoais no menor número de locais necessário. A equipa não deverá criar nenhum duplicado de Dados Pessoais se não for obrigada a fazê-lo por um motivo convincente;
- A equipa deve aproveitar todas as oportunidades para garantir que os Dados Pessoais de terceiros sejam mantidos atualizados. Por exemplo, se os dados pessoais do cliente foram alterados, tal pode ser confirmado através de uma chamada;
- Quem lida diretamente com o cliente deve poder atualizar os Dados Pessoais mantidos pelo Grupo Visabeira. As pessoas também devem poder solicitar atualizações aos seus dados pessoais facilmente, por exemplo, através do site da empresa;
- Os dados devem ser atualizados à medida que forem descobertas imprecisões. Por exemplo, se o número de um cliente for considerado incorreto, deverá ser retirado da base de dados;
- É responsabilidade do diretor de marketing garantir que as bases de dados de marketing sejam verificadas em relação aos arquivos de supressão do sector a cada seis meses.

### 10. Princípios gerais de privacidade observados pelo Grupo Visabeira

Os seguintes princípios gerais baseiam-se nos princípios do RGPD e na lei aplicável de proteção de dados da UE/EEE, onde se aplica. Mais detalhes podem ser definidos nos procedimentos gerais de privacidade de dados e segurança da informação, aplicáveis a todas as Unidades de Negócio.

**Legalidade, justiça e transparência**

Os Dados Pessoais serão tratados de forma justa, lícita, transparente e de acordo com os princípios estipulados nesta Política de Proteção de Dados (e quaisquer outras políticas relevantes do Grupo Visabeira).

**Limitação de finalidade**

Os Dados Pessoais devem ser recolhidos para fins específicos, explícitos e legítimos e não serão posteriormente tratados de forma incompatível com esses fins.

**Minimização de dados, precisão e limitação de armazenamento**

Os Dados Pessoais devem ser:

- (a) Adequados, relevantes e limitados ao essencial relativamente às finalidades para as quais são recolhidos e/ou processados posteriormente (“minimização de dados”);
- (b) Exatos e, onde necessário, mantidos atualizados; devem ser tomadas todas as medidas possíveis para garantir que dados incorretos, tendo em conta as finalidades para os quais foram recolhidos ou processados posteriormente, sejam apagados ou retificados de imediato (“exatidão”); e
- (c) Mantidos de forma que seja possível a identificação dos Titulares dos Dados por um período nunca superior ao necessário para os fins para os quais os dados foram recolhidos ou para os quais sejam posteriormente processados (“limitação de armazenamento”).

**Processamento Legal dos Dados Pessoais**

Os Dados Pessoais devem ser processados apenas quando um ou mais dos seguintes requisitos legais se aplicam:

- (a) O Titular dos Dados deu o seu Consentimento para o Tratamento dos seus Dados Pessoais para uma ou mais finalidades específicas;
- (b) O Processamento é necessário para a execução de um contrato no qual o Titular dos Dados seja uma das partes interessadas, ou de modo a tomar medidas a pedido do Titular dos Dados antes da celebração de um contrato;
- (c) O Processamento for necessário para o cumprimento de uma obrigação legal a que o Responsável pelo Tratamento esteja sujeito;
- (d) O Processamento for necessário para proteger os interesses vitais do Titular dos Dados ou de outra pessoa singular;

- (e) O Processamento for necessário para o desempenho de uma tarefa realizada no interesse público ou no exercício da autoridade oficial investida no Responsável pelo Processamento; ou
- (f) O Processamento for necessário para efeitos dos interesses legítimos pretendidos pelo Responsável pelo Tratamento ou por terceiros, exceto quando esses interesses forem sobrepostos pelos interesses ou direitos e liberdades fundamentais do Titular dos Dados, que exijam a proteção dos seus Dados Pessoais.

### **Processamento de Dados Sensíveis**

Normalmente, o Processamento de Dados Sensíveis é proibido, ou seja, Dados Pessoais que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, ou o Processamento de dados genéticos, dados biométricos com a finalidade de identificação única de uma pessoa singular, dados relativos à saúde, vida sexual ou orientação sexual. Os Dados Sensíveis só podem ser processados se:

- (a) O Titular dos Dados der o seu consentimento explícito para o processamento desses dados para um ou mais fins específicos, exceto quando as leis locais aplicáveis à Unidade de Negócio estabelecerem que a proibição acima não pode ser levantada pelo Titular dos Dados;
- (b) O Processamento for necessário para efeitos de cumprimento das obrigações e exercício de direitos específicos do Responsável pelo Tratamento ou do Titular dos Dados no domínio da lei do trabalho, da segurança social e da proteção social, na medida em que seja autorizado pela legislação local ou por um acordo coletivo nos termos da legislação local que preveja salvaguardas adequadas para os direitos fundamentais e os interesses do Titular dos Dados;
- (c) O Processamento for necessário para proteger os interesses vitais do Titular dos Dados ou de outra pessoa singular quando o Titular dos Dados esteja física ou legalmente incapaz de dar o seu Consentimento;
- (d) O Processamento disser respeito a dados que são manifestamente tornados públicos pelo Titular dos Dados;
- (e) O Processamento for necessário para o estabelecimento, exercício ou defesa de ações legais ou sempre que os tribunais agirem no exercício das suas funções judiciais;
- (f) O Processamento for necessário para fins de medicina preventiva ou ocupacional, para avaliação da capacidade de trabalho do colaborador, diagnóstico médico, prestação de cuidados de saúde, assistência social, tratamento ou gestão de sistemas de saúde ou assistência social e serviços com base na legislação local ou ao abrigo de um contrato

com um profissional de saúde sujeito a sigilo profissional ou outra pessoa sujeita ao mesmo tipo de sigilo; ou

- (g) O Processamento for permitido de acordo com as regras nacionais diferentes de (a) a (f) acima, e quando as regras nacionais tiverem sido estabelecidas de acordo com o RGPD.

### Condições para o consentimento

Se o Consentimento for permitido ou exigido no âmbito do RGPD para o Processamento de Dados Pessoais ou de Dados Sensíveis, aplicam-se as seguintes condições:

- (a) O Grupo Visabeira tem de ser capaz de demonstrar que obteve o consentimento do Titular dos Dados para o Processamento dos seus Dados Pessoais de forma informada, voluntária e especificada;
- (b) O Grupo Visabeira tem de garantir o seguinte, relativamente a qualquer Consentimento que obtenha:
- i) Se o Consentimento do Titular dos Dados for concedido no âmbito de uma declaração escrita que também diga respeito a outros assuntos, o pedido de Consentimento deve, sempre que a lei aplicável o exija, ser apresentado de forma claramente distinta dos demais assuntos, de forma inteligível e de fácil acesso, utilizando uma linguagem clara e simples; e
- ii) O Consentimento só deve ser utilizado quando for provável que seja válido como base legal para o Processamento. Relativamente às relações de emprego, o Consentimento não deve, portanto, ser utilizado como base legal, a menos que seja evidente que é concedido de forma voluntária. Normalmente, tal acontece quando os Titulares dos Dados participam voluntariamente de uma pesquisa ou de eventos organizados pelo Grupo Visabeira ou se registam para receber uma Newsletter interna do Grupo Visabeira;
- (c) O Titular dos Dados pode retirar o seu Consentimento a qualquer momento e deve, quando a lei aplicável assim o exigir, ser informado sobre o seu direito de retirar o seu Consentimento. Retirar o Consentimento não afetará a legalidade do Processamento com base em tal Consentimento antes de este ser retirado. Deverá ser tão fácil retirar como dar consentimento.



### **Procedimento para lidar com as solicitações do Titular de Dados**

Antes de atender à solicitação de um Titular de Dados para exercer um direito de proteção de dados, o Responsável pelo Processamento deve solicitar prova da identidade do indivíduo. Uma vez verificada a sua identidade, o Responsável pelo Processamento não deve demorar a responder ao pedido. O Responsável pelo Processamento pode solicitar mais detalhes ao Titular dos Dados sobre a solicitação (por exemplo, se o Titular dos Dados está ciente das circunstâncias em que o Responsável pelo Processamento obteve os Dados Pessoais ou os sistemas nos quais os Dados Pessoais relevantes provavelmente serão armazenados).

Quando a solicitação for feita através de um meio eletrónico, a resposta será fornecida da mesma forma sempre que possível (desde que o meio seja seguro), salvo pedido em contrário do Titular dos Dados. O pedido deve ser respondido sem demora injustificada e, em qualquer caso, no prazo de um mês a contar da data de receção do pedido. O referido prazo poderá ser prorrogado por mais dois meses, se necessário, tendo em conta a complexidade do pedido. Nesses casos, o Titular dos Dados será informado de tal prorrogação no prazo de um mês a contar da receção do pedido, juntamente com os motivos para tal atraso.

No caso de uma objeção, o *Data Protection Officer* (Responsável pela Proteção de Dados) responderá confirmando se o Processamento específico será interrompido ou não. Se o Processamento não for interrompido, a comunicação deve ser acompanhada dos motivos para continuar o Processamento.

### **Confidencialidade do Processamento**

Qualquer pessoa agindo sob a autoridade do Responsável pelo Processamento ou do Processador, incluindo o próprio Processador, que tenha acesso aos Dados Pessoais não deve processá-los, exceto sob as orientações do Responsável do Processamento, a menos que seja obrigado a fazê-lo por lei.

### **Responsáveis Conjuntos**

Nas situações em que dois ou mais Responsáveis pelo Processamento determinam conjuntamente os propósitos e meios do Processamento, eles serão considerados Responsáveis Conjuntos. Tais situações podem surgir quando duas Unidades de Negócio determinam juntas as finalidades e os meios do Processamento, o que pode ser o caso, por exemplo, em projetos de pesquisa conjuntos.

O facto de dois ou mais Responsáveis pelo Processamento serem Responsáveis pelo Processamento Conjunto deve ser avaliado caso a caso e depende da existência ou não de determinação conjunta em relação aos propósitos e meios do Processamento. Nos casos de

Responsáveis Conjuntos, eles devem determinar de maneira transparente as suas respectivas responsabilidades pelo cumprimento da legislação de proteção de dados da UE/EEE aplicável, em particular no que diz respeito aos requisitos de informação e aos direitos dos Titulares dos Dados.

As respectivas responsabilidades das partes devem ser descritas num acordo entre as partes, nomeadamente no que diz respeito ao exercício dos direitos do Titular dos Dados e respectivas obrigações em facultar a informação. Além disso, por norma o acordo deve incluir:

- descrição do mapa de processamento e fluxo de dados;
- as responsabilidades das partes no que respeita ao cumprimento da proteção de dados;
- divulgação de dados e confidencialidade;
- medidas de segurança tecnológica e organizacional e realização de avaliação de risco;
- uso de subcontratados;
- transferências de dados para Países Terceiros;
- eliminação e devolução de dados;
- aplicabilidade de procedimentos internos;
- responsabilidade.

A essência do acordo deve ser disponibilizada ao Titular dos Dados e deve refletir devidamente as respectivas funções das partes e as relações dos Responsáveis Conjuntos com os Titulares dos Dados.

#### **Utilização de processadores de dados**

Quando o Grupo Visabeira estiver sujeita ao RGPD e a contratos com prestadores de serviços para a prestação de serviços que envolvam o Processamento de Dados Pessoais pelo Grupo Visabeira, apenas serão escolhidos os Processadores que forneçam garantias suficientes para implementar medidas técnicas e organizacionais, de forma que o Processamento cumpra os requisitos do RGPD.

O Processamento por um Processador será regido por um contrato (um Acordo de Processamento de Dados) que, no mínimo, estabeleça o objeto e a duração do Processamento, a sua natureza e finalidade, o tipo de Dados Pessoais e as categorias dos Titulares dos Dados e as obrigações e direitos do Responsável pelo Processamento. O contrato deve estipular, em particular, que o Processador:

- (a) Processa os Dados Pessoais apenas mediante instruções documentadas do Responsável pelo Processamento, inclusive no que diz respeito a transferências de Dados Pessoais

- para um País Terceiro ou uma organização internacional, a menos que tal seja exigido pela legislação nacional à qual o Processador está sujeito; nesse caso, o Processador informará o Responsável pelo Processamento desse requisito legal antes de efetuar o Processamento, a menos que a lei proíba tais informações por motivos importantes de interesse público;
- (b) Garante que as pessoas autorizadas a Processar os Dados Pessoais se comprometem com a sua confidencialidade ou se encontrem sob adequada obrigação legal de confidencialidade;
  - (c) Toma todas as medidas exigidas por lei relacionadas com a segurança do Processamento;
  - (d) Respeita as condições abaixo mencionadas relacionadas com a contratação de outro Processador;
  - (e) Tendo em consideração a natureza do Processamento, auxilia o Responsável pelo Processamento através de medidas técnicas e organizacionais adequadas, na medida do possível, para o cumprimento da obrigação por parte do Responsável pelo Processamento em responder a solicitações para exercer os direitos do Titular dos Dados, no âmbito da lei de proteção de dados da UE/EEE que seja aplicável;
  - (f) Auxilia o Responsável pelo Processamento no cumprimento das obrigações legais relacionadas com a segurança do Processamento e com a consulta às Autoridades de Supervisão, tendo em consideração a natureza do Processamento e as informações disponíveis para o Processador;
  - (g) À escolha do Responsável pelo Processamento, exclui ou devolve todos os Dados Pessoais após terminar a prestação de serviços relacionada com o Processamento e apaga as cópias existentes, a menos que a lei aplicável exija o armazenamento dos Dados Pessoais;
  - (h) Disponibiliza ao Responsável pelo Processamento todas as informações necessárias para o cumprimento das obrigações previstas nesta Política de Proteção de Dados e permiti e contribui para a realização de auditorias, incluindo inspeções, levadas a cabo pelo Responsável pelo Processamento ou outro auditor por ele nomeado. O Processador não deve contratar outro Processador sem autorização prévia por escrito, específica ou geral, do Responsável pelo Processamento. No caso de uma autorização geral por escrito, o Processador deve informar o Responsável pelo Processamento de quaisquer alterações pretendidas relativamente ao acréscimo ou substituição de outros Processadores, dando assim ao Responsável pelo Processamento a oportunidade de se opor a tais alterações.

**Proteção de dados por desenho e por omissão.**

O Responsável pelo Processamento deverá, quer ao determinar os meios de Processamento quer aquando do Processamento, implementar medidas técnicas e organizacionais adequadas, que visam implementar princípios de proteção de dados, como a minimização de dados, de maneira eficaz, de modo a integrar as garantias necessárias ao Processamento para proteger os direitos dos Titulares dos Dados.

O Responsável pelo Processamento deve implementar medidas técnicas e organizacionais apropriadas para garantir que, por regra, apenas os Dados Pessoais necessários para cada finalidade específica do Processamento sejam processados.

Esta obrigação aplica-se à quantidade de Dados Pessoais recolhidos, à extensão do seu Processamento, ao período do seu armazenamento e à sua acessibilidade. Em particular, estas medidas devem garantir que, por regra, os Dados Pessoais não sejam disponibilizados sem intervenção junto de um número indefinido de pessoas. Por favor, consulte o procedimento do Grupo Visabeira aplicável a esses princípios.

**Notificação de Violação de Dados Pessoais**

Caso tenha ocorrido ou se suspeite que tenha ocorrido uma Violação de Dados Pessoais, a pessoa que tiver conhecimento ou suspeitar da Violação de Dados Pessoais, deverá notificar imediatamente o respetivo responsável ou o DPO, que encaminhará o incidente para a Comissão de Segurança e Privacidade do Grupo (CSP).

Uma Violação de Dados Pessoais ocorre, por exemplo, se os sistemas de dados do Responsável pelo Processamento forem *hackeados*, os Dados Pessoais forem acidentalmente ou intencionalmente enviados para o destinatário errado, os Dados Pessoais forem deixados num local onde pessoas não autorizadas os possam aceder, roubo de dados e outros tipos de fuga de dados.

O Grupo Visabeira documentará quaisquer Violações de Dados Pessoais, compreendendo os factos relativos à Violação de Dados Pessoais, os seus efeitos e as medidas corretivas tomadas. Essa documentação deve ser disponibilizada à Autoridade de Proteção de Dados competente mediante solicitação.

## 11. Transferências

### Transferência de Dados Pessoais para Responsáveis pelo Processamento e Processadores que são membros do grupo (transferência interna)

#### Transferência entre Responsáveis pelo Processamento

A transferência de Dados Pessoais entre Responsáveis pelo Processamento pode ocorrer, desde que:

- (a) Não seja incompatível com a finalidade para a qual os Dados Pessoais foram recolhidos;
- (b) esteja de acordo com o princípio de minimização, precisão e limitação de armazenamento;
- (c) Os critérios para tornar legal o Processamento de dados sejam cumpridos (por exemplo, que uma base legal, como interesses legítimos, tenha sido identificada);
- (d) Se aplicável, as informações sejam fornecidas ao Titular dos Dados (por exemplo, com notificações de privacidade),
- (e) Medidas de segurança apropriadas protejam os dados durante a transferência e processamento posterior pelo Responsável pelo Processamento recetor; e
- (f) Se a transferência for de um Responsável pelo Processamento estabelecido no EEE para um Responsável pelo Processamento de um País Terceiro, deverão ser cumpridos os requisitos abaixo indicados.

A legislação local aplicável pode ter requisitos adicionais e deve sempre ser tida em consideração antes de se fazerem as referidas transferências.

#### Transferência para Processadores fora do EEE

A transferência de Dados Pessoais de um Responsável pelo Processamento estabelecido no EEE para um Processador num País Terceiro é proibida, exceto se forem cumpridas todas as condições, bem como uma das bases legais dos Artigos 45º, 46º, 47º ou 49º do RGPD, incluindo (a título de exemplo):

- (a) A transferência é regida por Regras Corporativas Vinculativas aprovadas, ou por um mecanismo de transferência semelhante que forneça as garantias adequadas de acordo com a lei aplicável;
- (b) O Responsável pelo Processamento e o Processador facultaram as garantias adequadas ao celebrar Cláusulas Contratuais Padrão da UE (contrato modelo);
- (c) Esteja previsto um código de conduta aprovado ou um mecanismo de certificação aprovado de acordo com o artigo 46 (1) (e) e (f) do RGPD.

## 12. Alterações à Política Interna de Proteção de Dados

Uma cópia integral desta Política Interna de Proteção de Dados pode ser obtida, digitalmente, no Portal Interno do Grupo Visabeira (*MyVisabeira – Corporate Intranet*) e no *site* do Grupo Visabeira.

Para que este documento seja mais eficaz, não estão previstas alterações significativas, no entanto, por uma questão de detalhe, O Grupo Visabeira reserva-se o direito de atualizar esta **Política de Proteção de Dados**, em qualquer altura, sendo todas as alterações consideradas efetivas a partir da data da sua publicação. Todos os colaboradores e demais pessoas interessadas serão informados sobre futuras alterações materiais.

|            |                               |
|------------|-------------------------------|
| Documento: | Política de Proteção de dados |
| Versão:    | 1.0                           |
| Data:      | Julho 2024                    |