



Política de Proteção de Dados

Introdução

No desenvolvimento da sua atividade a JHFLopes mantém um registo de dados pessoais sobre os seus funcionários, clientes, fornecedores e outros titulares de dados.

A JHFLopes está empenhada em proteger os direitos e liberdades dos titulares de dados, processar os seus dados de forma segura e de acordo com todas as obrigações legais.

Esta política define a forma como protegemos os dados pessoais e assegura que os nossos funcionários entendem as regras que regem o uso dos dados pessoais a que têm acesso no decorrer de seu trabalho.

Esta política assegura que o Diretor de Proteção de Dados (DPO) seja consultado antes que qualquer nova atividade significativa de processamento de dados seja iniciada para garantir que as etapas de conformidade relevantes sejam abordadas.

Definições

Fins operacionais	<p>Os fins para os quais os dados pessoais podem ser usados para:</p> <p>Desenvolvimento de pessoal, administrativo, financeiro, regulatório, folha de pagamento e desenvolvimento de negócios.</p> <p>Os propósitos de negócios incluem o seguinte:</p> <ul style="list-style-type: none">• Cumprimento de obrigações legais, regulatórias e boas práticas.• Em resposta a solicitações de autoridades de segurança.• Garantir que as políticas da empresa são seguidas (como políticas de segurança, de e-mail e internet entre outras).• Averiguação de queixas, reclamações e auditorias.• Verificação de referências, garantia de práticas seguras de trabalho, vigilância e gestão do acesso do pessoal a sistemas e instalações e ausências, administração e avaliações do pessoal.• Acompanhamento da conduta do pessoal, questões disciplinares.• No desenvolvimento da atividade de Despachante, nomeadamente nas atividades de importação/exportação, matriculação e legalização de veículos automóveis.
Dados pessoais	<p>informação relativa a uma pessoa singular identificada ou identificável («titular dos dados») - é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.</p>
Categorias especiais de dados pessoais	<p>As categorias especiais de dados incluem informação de uma pessoa singular sobre a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.</p>
Responsável pelo tratamento	<p>A pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.</p>
Subcontratante	<p>Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.</p>

Tratamento	<p>Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.</p>
Autoridade de controlo	<p>Autoridade pública independente criada por um Estado-Membro nos termos do artigo 51º. A Autoridade de controlo para a nossa organização é a CNPD - Comissão Nacional de Proteção de Dados (www.cnpd.pt).</p> <p>A CNPD é considerada a autoridade de controlo, quando, nomeadamente, o país da residência do titular dos dados for Portugal, bem como nos casos em que, existindo um tratamento de dados pessoais que englobe vários países, o responsável (ou o Subcontratante) tiver o seu estabelecimento principal em Portugal.</p>

Âmbito

Esta política aplica-se a todos os funcionários, que devem estar familiarizados com esta política e cumprir com os seus termos.

Esta política pode, a qualquer momento, ser complementada ou alterada por políticas e diretrizes adicionais. Qualquer política, nova ou modificada, será distribuída por todos os funcionários antes de ser implementada.

Quem é responsável por esta política?

O nosso Diretor de Proteção de Dados (DPO), Carlos Bernardo é o responsável pela implementação geral desta política. O DPO deve ser contactado sempre que necessitar de mais informação, ou esclarecer eventuais dúvidas, sobre esta política.

Contatos:

Correio eletrónico: rgpd@jhflopes.com

Morada: Rua Terreiro do Trigo, 66 - 4B - 1149-062 - Lisboa

Princípios

A JHFLopes deve cumprir os princípios de proteção de dados enumerados no Regulamento Geral de Proteção de Dados (UE) 2016/679 (“RGPD”). Faremos todos os esforços possíveis para cumprir com estes princípios. Os Princípios são:

1. Licitude, lealdade e transparência

Os dados são objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados.

2. Limitação das finalidades

Os dados são recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades.

3. Minimização dos dados

Os dados recolhidos são adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados.

4. Exatidão

Os dados recolhidos são exatos e atualizados sempre que necessário.

5. Limitação da conservação

Os dados são conservados numa forma que permita a identificação dos titulares apenas durante o período necessário para as finalidades para as quais são tratados.

6. Integridade e Confidencialidade

Os dados são tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adotando as medidas técnicas ou organizativas adequadas (MTO).

Responsabilização e Transparência

Devemos garantir, recorrendo ao registo das atividades de processamento, que a utilização de dados pessoais é feita de forma transparente e responsável e devemos demonstrar que cumprimos cada princípio. Este registo será mantido atualizado e deve ser aprovado pelo DPO.

Para garantir a conformidade com estes princípios, cada funcionário é responsável por entender as suas responsabilidades específicas para garantir que cumprimos as seguintes obrigações de proteção de dados:

- Implementar todas as medidas técnicas e organizacionais (MTO) apropriadas.
- Manter um registo atualizado sobre todas as atividades de processamento relevantes.
- Efetuar Avaliações de Impacto sobre Proteção de Dados (DPIA).
- Garantir a implementação de medidas que assegurem a privacidade desde a conceção (design) e por defeito (default), incluindo:
 - Minimização dos dados.
 - Pseudonimização.

- Transparência.
- Permitir a monitorização do processamento.
- Implementar e melhorar os procedimentos de segurança e privacidade de forma contínua.

Procedimentos

Processamento lícito e justo

Devemos efetuar o processamento de dados pessoais de forma lícita e justa, de acordo com os direitos dos indivíduos do primeiro Princípio (**Licitude, lealdade e transparência**). Isso geralmente significa que não devemos processar dados pessoais sem que o indivíduo tenha dado o seu consentimento.

Se ilícito (explicado abaixo) o nosso processamento não está de acordo com o primeiro Princípio e é ilegal. Neste caso os titulares dos dados têm o direito de ter quaisquer dados processados ilegalmente apagados.

Responsabilidade vs. processamento de dados

A JHFlopes é simultaneamente **Responsável pelo tratamento** de dados e **Subcontratante**.

Como Subcontratante devemos cumprir as nossas obrigações contratuais e agir de acordo com as instruções escritas do responsável pelo tratamento. Se em algum momento determinarmos o propósito do tratamento e alterarmos as instruções do responsável pelo tratamento, seremos considerados responsáveis pelo tratamento de dados, violando o contrato que temos com o responsável pelo tratamento e assumindo igual responsabilidade. Como Subcontratante, devemos:

- Obter autorização escrita do responsável pelo tratamento antes de recorrer a Subcontratantes.
- Cooperar de forma plena com a Autoridade de Controlo.
- Garantir o processamento seguro dos dados.
- Manter um registo atualizado das atividades de processamento de dados.
- Comunicar qualquer violação de dados pessoais ao responsável pelo tratamento de dados.

Se tiver alguma dúvida sobre a forma como lidamos com os dados pessoais deve entrar em contato com o DPO para obter esclarecimentos.

Licitude do tratamento

O processamento de dados só pode ser efetuado se tiver uma base legal. Certifique-se de que quaisquer dados que processa têm uma base legal aprovada pelo DPO. É da sua responsabilidade verificar a base legal dos dados que processa e garantir que todas as suas ações cumprem a legislação em vigor. Pelo menos uma das seguintes condições deve ser aplicada sempre que processarmos dados pessoais:

Consentimento

Temos o consentimento, claro, explícito e definido para que os dados do indivíduo sejam processados com uma, ou mais, finalidades específicas.

Contrato

O processamento é necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados.

Obrigação jurídica

Cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito (sem contrato).

Interesses vitais

O processamento é necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular.

Interesse público

Quando o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública.

Interesses legítimos

Quando o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros. Esta condição não se aplica se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Aferir a licitude do tratamento

Cada funcionário deve decidir se o tratamento é necessário antes de avaliar a sua licitude. Isso significa que o processamento deve ser efetuado de forma a atingir o objetivo declarado. Podem ser aplicadas várias condições na avaliação da licitude do tratamento, no entanto deve escolher a que melhor se ajusta ao propósito, e não a que é mais fácil.

Considere as seguintes questões na sua avaliação:

- Qual é o objetivo do processamento dos dados?
- O processamento pode ser feito de uma maneira diferente?
- Existe uma escolha entre processar ou não os dados?
- Quem beneficia com o processamento?
- A base legal que escolheu é a mesma que o titular dos dados escolheria?
- Qual é o impacto do processamento no indivíduo?
- Está em posição de poder sobre o titular dos dados?
- O titular dos dados é uma pessoa vulnerável?
- O titular dos dados opõe-se ao processamento?

O nosso compromisso com o primeiro Princípio exige que documentemos os processos de tratamento de dados, qual a base legal aplicada ao objetivo de cada processo, e que justifiquemos plenamente essas decisões.

Devemos garantir que indivíduos cujos dados são processados sejam informados, por via de um aviso sobre a privacidade, sobre a licitude e finalidade do tratamento. Esta informação deve ser prestada quando os dados são obtidos diretamente do indivíduo ou de outra fonte.

A avaliação da licitude do tratamento e implementação do aviso sobre privacidade deve ser aprovada pelo DPO.

Categorias especiais de dados

Os dados especiais são dados sensíveis que requerem mais proteção porque podem criar riscos mais significativos para os direitos e liberdades fundamentais de uma pessoa. As categorias especiais incluem informações de indivíduo sobre:

- Origem racial ou étnica.
- Opiniões políticas.
- Convicções religiosas e filosóficas.
- Filiação sindical.
- Dados genéticos.
- Dados biométricos usados para identificar uma pessoa de forma inequívoca.
- Dados relativos à saúde.
- Dados relativos à vida sexual ou orientações sexuais.

O processamento de categorias especiais de dados pessoais só pode ser realizado mediante o consentimento explícito do titular dos dados, exceto se tal for exigido por lei ou se apliquem as circunstâncias excepcionais previstas no RGDP.

O consentimento deve identificar claramente quais são os dados relevantes, o motivo do seu processamento e a quem serão divulgados.

O processamento de categorias especiais de dados pessoais deve estar em conformidade com a lei. As atividades de processamento devem terminar se não existir base legal para o processamento das categorias especiais de dados.

Responsabilidade

A JHFLopes é responsável por:

- Analisar e documentar os tipos de dados pessoais que possuímos.
- Verificar que os procedimentos de tratamento de dados cobrem todos os direitos do indivíduo.
- Assegurar a base legal para o processamento de dados.
- Garantir que os procedimentos de consentimento sejam lícitos.
- Implementar e rever os procedimentos de forma a detetar, relatar e investigar violações na utilização de dados pessoais.
- Armazenar dados de maneira segura e protegida.
- Avaliar o risco que pode ser colocado, aos direitos e liberdades individuais, caso os dados sejam comprometidos.

Os funcionários são responsáveis por:

- Compreender totalmente as suas obrigações ao nível da proteção de dados.
- Verificar se as atividades de processamento de dados em que estão envolvidos são justificadas e estão em conformidade esta política.
- Garantir que os dados não são processados de forma ilegal.
- Assegurar que as suas ações não comprometem a segurança dos dados, não violam as leis de proteção de dados, e a nossa política de proteção de dados.
- Cumprir com esta política em todos os momentos.
- Levantar quaisquer preocupações, notificar quaisquer violações ou erros e relatar imediatamente qualquer assunto suspeito ou contraditório que coloque em risco o cumprimento desta política e/ou as nossas obrigações legais.

O DPO é responsável por

- Manter a Direção informada sobre responsabilidades, riscos e problemas relacionados com a proteção de dados.
- Rever regularmente os procedimentos e políticas de proteção de dados.
- Organizar ações de formação e aconselhamento sobre o tema da proteção de dados.
- Responder a perguntas, dos funcionários, da Direção e outras partes interessadas, sobre a proteção de dados.
- Responder às questões colocadas pelos titulares dos dados, clientes e funcionários que desejam saber que dados são mantidos pela JHFLopes.
- Verificar e aprovar com terceiros quaisquer contratos ou acordos relativos ao processamento de dados.

O Diretor de TI é responsável por:

- Garantir que todos os sistemas, serviços, software e equipamentos cumprem padrões de segurança aceitáveis.
- Verificar de forma regular o correto funcionamento do hardware e software de segurança assegurando o seu correto funcionamento.
- Investigar serviços de terceiros, tais como serviços na nuvem, a que a JHFLopes possa recorrer para armazenar ou processar dados.

Precisão e relevância

Considerando o objetivo para o qual foram obtidos, garantimos que os dados pessoais que processamos são precisos, adequados, relevantes e não excessivos. Não processaremos dados pessoais com outra finalidade diferente daquela para que foram recolhidos.

Em caso de incorreção os indivíduos podem solicitar a retificação dos seus dados pessoais. O DPO deve ser informado caso sejam detetadas imprecisões ou no caso de eventuais disputas.

Segurança dos dados

Os dados devem ser protegidos contra perdas ou uso indevido. Se os dados forem processados por terceiros, o DPO deve, se necessário, definir que medidas de segurança adicionais deverão ser implementadas, e estas medidas devem constar nos contratos em vigor com as entidades terceiras.

Arquivo seguro de dados

- Os dados armazenados em papel impresso devem ser mantidos em local seguro acessível apenas por pessoas autorizadas.
- Os dados em papel impresso devem ser triturados quando deixarem de ser necessários.
- Os dados armazenados em computador devem ser protegidos por senhas fortes que sejam alteradas regularmente.
- Os dados armazenados em suportes moveis, tais como discos externos, Pens ou cartões de memória, devem ser encriptados, ou protegidos por senha, e guardados em segurança quando não estiverem a ser utilizados.
- O DPO deve aprovar qualquer armazenamento de dados na nuvem.
- Os servidores que contêm dados pessoais devem ser mantidos em local seguro - separados do espaço geral do escritório.
- Os dados devem ser copiados com regularidade de acordo com os procedimentos de backup da empresa.
- Os dados nunca devem ser salvos diretamente em dispositivos móveis, como portáteis, *tablets* ou *smartphones*, exceto situações aprovadas pelo DPO.
- Todos os servidores que contêm dados confidenciais devem ser aprovados e protegidos por software de segurança.
- Devem ser aplicadas as medidas técnicas possíveis e adequadas, para manter os dados seguros.

Retenção de dados

Os dados serão mantidos pelo período de tempo estritamente necessário. A determinação deste período dependerá de questões legais e contratuais e das circunstâncias de cada caso, considerando sempre as razões pelas quais os dados pessoais foram inicialmente obtidos.

Transferência internacional de dados

Existem restrições às transferências internacionais de dados pessoais. Estes não devem ser transferidos para o fora da UE, ou qualquer outro lugar que esteja fora das regras e procedimentos normais, sem a permissão expressa do DPO.

Direitos do titular dos dados

Os indivíduos têm direitos que devemos respeitar e cumprir dentro das nossas melhores capacidades. Garantimos o exercício destes direitos das seguintes formas:

1. Direito a ser informado

- Enviar avisos de privacidade que sejam concisos, transparentes, inteligíveis e de fácil acesso, gratuitos, escritos em linguagem clara e simples, especialmente se destinados a crianças.
- Manter um registo da utilização de dados pessoais em conformidade com a necessidade de responsabilidade e transparência.

2. Direito de acesso

- Permitir o acesso dos indivíduos aos seus dados pessoais e informações suplementares.
- Permitir que os indivíduos validem a licitude das atividades de processamento.

3. Direito de retificação

- Devemos corrigir os dados pessoais do indivíduo, se solicitado, quando estes estejam incorretos ou incompletos.
- Isso deve ser feito sem demora e no prazo máximo um mês. Este prazo poderá ser estendido para dois meses com a permissão do DPO

4. Direito de apagamento

- Não existindo razões para o seu processamento, devemos excluir ou remover os dados de um indivíduo quando solicitado.

5. Direito à limitação do tratamento

- Devemos cumprir qualquer solicitação para limitar, bloquear ou, de outra forma, interromper o processamento de dados pessoais.
- Se for solicitada a limitação de tratamento, estamos autorizados a armazenar os dados pessoais sem que seja possível o seu processamento. Devemos manter os dados suficientes para garantir que o direito à limitação de tratamento seja respeitado no futuro

6. Direito à portabilidade dos dados

- Quando solicitado devemos fornecer ao titular dos direitos os seus dados para que este possa reutilizá-los para os seus próprios fins ou entre diferentes serviços.
- Devemos fornecê-los num formato comumente legível por máquina e, se solicitado, enviá-los diretamente para outro Responsável pelo tratamento.

7. Direito de oposição

- O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, incluindo quando estes são utilizados para efeitos de comercialização direta.

8. Direito relativo a decisões automatizadas e definição de perfis

- O titular dos dados tem o direito de não estar sujeito a uma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

Informação ao titular

Quando fornecer um aviso de privacidade

Um aviso de privacidade deve ser fornecido após solicitação do titular ou no momento em que os dados são obtidos – se forem obtidos diretamente junto titular dos dados. Se os dados não forem obtidos junto do titular dos dados, o aviso de privacidade deve ser fornecido dentro de um período razoável, o mais tardar no prazo de um mês, após a obtenção dos dados.

Nos casos em que se preveja a divulgação dos dados a outro destinatário, o aviso de privacidade deve ser fornecido o mais tardar aquando da primeira divulgação.

Informação que deve constar do aviso de privacidade

Os avisos de privacidade devem ser concisos, transparentes, inteligíveis e de fácil acesso. Os avisos serão fornecidos sem qualquer custo e devem ser escritos em linguagem clara e simples, particularmente se forem destinados a crianças.

A informação seguinte deve ser incluída em todos os avisos de privacidade:

- Identificação e informações de contato do Responsável pelo processamento e, se for caso disso, do seu representante.
- As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento.
- Os interesses legítimos do responsável pelo tratamento ou de um terceiro.
- O direito de retirar o consentimento a qualquer momento, se aplicável.
- As categorias dos dados pessoais em questão (apenas para dados não obtidos diretamente junto do titular dos dados).
- Os destinatários ou categorias de destinatários dos dados pessoais, se os houver.
- Informação detalhada de quaisquer transferências para países terceiros e salvaguardas.
- O período de retenção dos dados ou os critérios usados para determinar o período de retenção, incluindo detalhes para a eliminação de dados após o período de retenção.
- O direito de apresentar reclamação a uma autoridade de controlo.
- A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público (apenas para dados não obtidos diretamente do titular dos dados).
- A existência de decisões automatizadas, incluindo a definição de perfis e informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
- Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados (somente para dados obtidos diretamente do titular dos dados).

Direito de acesso

O que é o direito de acesso?

O titular dos dados tem o direito de receber uma confirmação de processamento dos seus dados, o acesso aos seus dados pessoais e informações complementares. Estas informações devem se facultadas num aviso de privacidade.

Como responder a solicitações de acesso

Fornecemos gratuitamente ao titular dos dados uma cópia da informação, o mais tardar no prazo de um mês. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente.

Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos, devendo neste caso informar o titular dos dados de alguma prorrogação e dos motivos da demora no prazo de um mês a contar da data de receção do pedido. Antes da prorrogação do prazo deverá ser solicitada a aprovação do DPO.

Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu carácter repetitivo podemos:

- Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas.
- Não dar seguimento ao pedido.

Se não for dado seguimento ao pedido, o titular dos dados será informado sem demora do motivo, o mais tardar, no prazo de um mês a contar da data de receção do pedido, e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial.

Direito de portabilidade dos dados

O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um Responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro Responsável pelo tratamento.

Direito ao apagamento

O titular dos dados tem o direito a ter os seus dados apagados e o processamento termina nas seguintes circunstâncias:

- Quando os dados pessoais deixam de ser necessários para a finalidade para a qual foram originalmente recolhidos e / ou processados.
- Quando o consentimento é retirado.
- Quando o titular dos dados se opor ao processamento e não existir interesse legítimo na sua manutenção.
- Os dados pessoais foram processados ilegalmente ou infringiram as leis de proteção de dados.
- Para cumprir uma obrigação legal
- O processamento diz respeito a uma criança

Se dados pessoais que devem ser apagados foram transmitidos a outras entidades, estes devem ser informados da sua obrigação de apagar os dados. Se o titular dos dados o solicitar, deve ser informado sobre quem são esses destinatários.

Direito de oposição

O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito. O tratamento dos dados pessoais deve terminar a menos que:

- Existam razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados.
- Ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

O titular dos dados deve ser informado deste direito, se possível, no momento de recolha dos dados.

Direito a restringir decisões automatizadas e definição de perfis

Decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na esfera jurídica do titular de direitos ou que o afete significativamente de forma similar só podem ser efetuadas nas seguintes circunstâncias:

- Quando for necessária para a celebração ou a execução de um contrato.
- Com base no consentimento explícito do indivíduo.
- Quando autorizado por lei.

Nestas circunstâncias, devemos:

- Dar aos indivíduos informações detalhadas sobre o processamento automatizado.
- Simplificar a solicitação de intervenção humana ou a contestação de uma decisão.
- Realizar auditorias para garantir que os nossos sistemas cumprem os requisitos do RGDP.

Terceiros

Como Responsáveis pelo tratamento e/ou Subcontratantes devemos ter em vigor contratos escritos com terceiros a que recorreremos. O contrato deve conter cláusulas específicas que estabeleçam as obrigações e responsabilidades de ambas as partes.

Enquanto Responsáveis pelo tratamento apenas devemos recorrer a Subcontratantes que forneçam garantias suficientes sob o cumprimento do RGPD e assegurem o cumprimento, respeito e proteção dos direitos dos titulares de dados.

Como Subcontratantes devemos agir de acordo com as instruções escritas no contrato celebrado com o Responsável pelo processamento, cumprindo os requisitos do RGPD e o cumprimento, respeito e proteção dos direitos dos titulares de dados.

Contratos

Os nossos contratos devem cumprir os padrões estabelecidos pela Autoridade de Controlo. O contrato com Responsáveis pelo tratamento e/ou Subcontratante deve definir o objeto e a duração do processamento, a natureza e a finalidade das atividades de processamento, os tipos de dados pessoais e categorias de dados e as obrigações e direitos do Responsável pelo tratamento dos dados.

No mínimo, nossos contratos devem incluir cláusulas que especifiquem:

- O cumprimento das instruções escritas.
- Os envolvidos no processamento dos dados estão sujeitos a um dever de confiança.
- A utilização de MTO para garantir a segurança do processamento.
- Só serão contratados Subcontratantes com consentimento prévio do controlador e sob um contrato escrito.
- Que o Responsável pelo tratamento ajudará o Subcontratante a lidar com as solicitações de acesso e permitirá que os titulares de dados exerçam os seus direitos de acordo com o RGPD.
- Que o Subcontratante ajudará o Responsável pelo tratamento no cumprimento das suas obrigações do RGPD, nomeadamente em relação à segurança do processamento, notificação de violações de dados e realização de Avaliações de Impacto de Proteção de Dados (DPIA).
- Apagar ou devolver todos os dados pessoais no final do contrato.
- A autorização para realização de auditorias e inspeções regulares e fornecer as informações necessárias para que o Responsável pelo tratamento e o Subcontratante cumpram suas obrigações legais.
- Que nada será feito pelo Responsável pelo tratamento ou Subcontratante para violar o GDPR.

Condenações penais e infrações

Registos criminais

Embora previsto na lei, o tratamento de dados pessoais relacionados com condenações penais e infrações só pode ser efetuado se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados.

Os dados pessoais relacionados com condenações penais e infrações são considerados uma categoria especial, sendo necessário obter autorização do DPO antes de se proceder à verificação de registos criminais.

Auditoria, Monitorização e Formação

Auditorias sobre a proteção de dados

Serão realizadas auditorias sobre a proteção de dados. Os resultados dessa verificação serão comunicados à Administração, devendo também ser facultados, quando solicitado, à autoridade de controlo competente.

As auditorias sobre a proteção devem reunir informações sobre os dados são que mantidos, onde são armazenados, como são usados, quem são responsáveis e quais os regulamentos ou períodos de retenção mais relevantes.

Estas devem ter um carácter regular, conforme definido pelo DPO e pelos procedimentos em vigor, para testar e avaliar a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Monitorização

Esta política deve ser respeitada por todos, sem exceção, a todo o momento. O DPO tem a responsabilidade geral sobre esta política. Esta política será sujeita a revisões e será retificada ou alterada conforme necessário.

Sempre que detetadas as violações desta devem ser comunicadas ao DPO.

Formação

Cada funcionário receberá formação, adequada às suas funções, sobre as disposições da lei de proteção de dados específica para sua função. Deve requerer nova ação de formação sempre que as suas funções e responsabilidades sejam alteradas.

As questões e solicitações sobre a proteção de dados, devem ser remetidas para o DPO.

Notificação

Qualquer violação desta política ou da lei de proteção de dados (RGDP) deve ser reportada logo que possível. Ou seja, assim que tomar conhecimento de uma violação. A JHFlopes está legalmente obrigada a comunicar qualquer violação de dados a CNPD em 72 horas.

Todos temos a obrigação de comunicar as não conformidades, reais ou potenciais, na proteção de dados pessoais (RGPD).

Esta obrigação permite-nos:

- Investigar a falha e adotar medidas corretivas, se for necessário.
- Manter um registo de falhas de conformidade.
- Notificar a CNPD sobre eventuais violações do RGPD.

Quem tenha conhecimento de uma violação, concreta ou potencial, desta política ou do incumprimento do RGDP, e não a comunique ao DPO poderá ser alvo de um procedimento disciplinar.

Incumprimento

Esta política deve ser levada a muito a sério porque o seu incumprimento coloca-o a si e à organização em risco.

Esta política é tão importante que o não cumprimento de qualquer requisito significa que JHFlopes poderá ser processada legalmente, o que poderá ter impactos sérios na continuidade da sua atividade, e que a título pessoal poderá levar à sua demissão.

Quaisquer dúvidas ou preocupações sobre qualquer assunto desta política, deverá entrar em contato com o DPO.