POLÍTICA DE DADOS PESSOAIS PARA PRESTADORES DE SERVIÇOS

Controlo de versões			
Versões	**Data de Validação**	**Editor**	**Modificações**
V0	1 de Dezembro de 2020	DPO team	Creation

F.INICIATIVAS, Consultadoria e Gestão Lda. com capital social de 100.000,00€
NIF: 508 643 759
Rua da Alfândega, Nº 108 – 1º Esquerdo
1100-016 Lisboa

Para qualquer dúvida, não hesite em contactar o Data Protection Officer (DPO): dpo-pt@fi-group.com

1.Introdução

A FI GROUP é uma empresa especializada em financiamentos de inovação e compromete-se a respeitar as obrigações que permitem a proteção de dados pessoais.

Desde a implementação da Regulamento Geral de Proteção de Dados (RGPD) n°2016/679, que entrou em vigor a 24 de Maio de 2016, as entidades legais que processam dados pessoais devem implementar as medidas necessárias para cumprir com o RGPD aplicável a partir de 25 de Maio de 2018, e a sua transposição para a lei nacional de cada país da UE.

Através da capacitação de pessoas que processam os Dados Pessoais, a Regulação visa reforçar a proteção e os direitos daqueles que são afetados pelo tratamento de dados pessoais.

Sob esta Regulação, a FI Group que tem acesso a dados pessoais deve agir como Responsável pelo tratamento.
Nas suas relações como prestadores de serviço/ou fornecedores que requerem comunicação de Dados Pessoais devem agir como Subcontratante.

Para cumprir com as suas obrigações, a FI Group tem a possibilidade de receber assistência dos seus Subcontratantes, que devem garantir a segurança dos dados pessoais que lhe foram confiados. Como tal, o Subcontratante pode apenas processar dados transmitidos no âmbito das instruções dadas pelo Responsável pelo Tratamento, sem prejuízo de disposições especificas que podem ser assinadas.

O propósito da Política de Dados Pessoais para prestadores de serviço é permitir que a FI Group enquanto Responsável pelo Tratamento possa comunicar aos seus subcontratantes as instruções a serem seguidas para o uso de dados pessoais que lhes foram confiados.

2. Informação Geral

ARTIGO 1 - DEFINIÇÕES

1. **Decisão de Adequação:** Um estatuto concedido pela Comissão Europeia a países fora do Espaço Económico Europeu (EEE) que proporciona um nível de proteção de Dados Pessoais comparável ao nível previsto pela lei europeia. Quando este estatuto é atribuído a um país, os Dados Pessoais podem passar livremente entre este e o EEE sem necessidades de outras salvaguardas.

2. **Apêndice à Política**: A Política inclui um apêndice que permite a identificação e a descrição dos Dados Pessoais confiados como parte do Serviço prestado no acordo contractual. Este Apêndice à Política é, como princípio, incorporado no acordo contractual e completado pelo Subcontratante e a FI Group.

3. **Política:** Uma política de Dados Pessoais para prestadores de serviço, daqui em Diante designada de "Política"

4. **CNPD: "**Comissão Nacional de proteção de Dados", a autoridade portuguesa de supervisão, cuja missão é proteger os dados pessoais e monitorizar as aplicações corretas do RGPD e a lei de dados pessoais implementadas.

5. **Dados Pessoais:** », 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;

6. **Acordo Contratual**: Uma cotação, um contrato de serviços ou qualquer acordo escrito que descreva a relação comercial entre o Subcontratante e a FI Group, à qual esta Política deve ser anexada.

7. **Falha de Segurança:** Fraqueza no sistema de segurança e proteção dos Dados Pessoais, que permite que uma pessoa prejudique a integridade deste sistema de proteção, a confidencialidade, ou a integridade dos dados protegidos. Uma falha de segurança não resulta automaticamente numa Falha de Dados Pessoais.

8. **Dia útil:** Dia(s) desde Segunda a Sexta-feira, inclusive, excluindo feriados.

9. **LEI DA PROTEÇÃO DE DADOS PESSOAIS correspondente à Lei n.º 58/2019, de 08 de Agosto:** 08 de Agosto de 2019, que Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

10. **Serviço**: Tarefas executadas pelo Processador de Dados a pedido da FI Group, que requer o processamento de dados Pessoais.

11. **Relatório Detalhado:** O A pedido da FI Group, relatórios enviados pelo Processador de Dados à FI Group a descrever todas as medidas técnicas e organizacionais, implementadas pelo mesmo para garantir o nível de segurança adaptado aos Dados Pessoais.

12. **Registo de Falha de Segurança: I**nventário que lista a descrição e solução prestada a uma falha de segurança.

13. **Registo de Processamento de Dados:** Inventário que lista todos os Dados Pessoais processados e também a informação útil relacionada.
14. **Responsável pelo tratamento ou "FI Group",** 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.

15. **RGPD:** Regulação Geral de Proteção de Dados (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016, aplicada desde 25 de Maio de 2018.

16. **Subcontratante:** uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

17. **Relatório Simplificado:** Significa o sumário elaborado pelo Subcontratante na eventualidade de uma mudança no método de assegurar a segurança de Dados Pessoais durante a tarefa. O Subcontratante descreve as razões e consequências desta mudança.

18. **Tratamento:** 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;

19. **Terceiro:** a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais

20. **Violação: Acesso não autorizado a Dados Pessoais ou riscos de segurança, que causam por acidente ou maneiras ilícitas quer a destruição, perda, alteração, divulgação não autorizada de dados pessoais comunicados, que estão guardados ou processados de alguma forma.**

ARTIGO 2 – PROPÓSITO DESTA POLÍTICA

Esta Política tem como objetivo definir as condições sob as quais o Subcontratante se encarrega de executar, em nome do Responsável pelo Tratamento, as operações de processamento de dados pessoais confiadas como parte do Acordo Contratual.

O Subcontratante daqui em diante certifica-se que respeita a legislação atual e as instruções impostas pelo Responsável pelo Tratamento.

ARTIGO 3 – DURAÇÃO DAS OBRIGAÇÕES

Esta política deve aplicar-se durante a vigência do Acordo Contratual.

No fim do Acordo Contratual, por qualquer razão o Subcontratante compromete-se a:

- Arquivar apenas Dados Pessoais estritamente necessários no âmbito das obrigações legais. Após o término das obrigações legais, os Dados Pessoais devem ser destruídos, exceto por um pedido de devolução, que deve ser feito antes do fim do estatuto de limitações, especificando o meio e formato do registo.

- Aplicar as instruções acima a cada subcontratante e enviar certificados de arquivação/destruição por todos os Subcontratantes, incluindo os seus próprios certificados.

Se nenhuma obrigação legal ou regulamentar requisitar que o Subcontratante deve manter os Dados Pessoais armazenados, este último deve responsabilizar-se a destruí-los permanentemente no fim de todos ou parte do Acordo Contractual, ou a pedido do Responsável pelo Tratamento.
Após o término do Acordo Contratual, as obrigações devem permanecer em vigor.

Qualquer alteração das normas em vigor relativas ao tratamento de Dados Pessoais, que dê origem a um reforço das obrigações do Subcontratante, deve ser imediatamente implementada por este último, que confirmará estas alterações ao Responsável pelo Tratamento. Em caso de contradição devido a estas evoluções, as Partes devem reunir-se com o propósito de definir uma emenda à Política.

3. Informação e instruções no tratamento de dados pessoais

ARTIGO 4 – DADOS PESSOAIS REFERIDOS PELA POLÍTICA

Todos os Dados Pessoais comunicados ao Subcontratante no âmbito do Acordo Contratual devem respeitar a Política.

O Subcontratante deve comprometer-se a identificar, dentro do período de um (1) mês após a assinatura da Política, o tipo de Dados Pessoais transmitidos de acordo com o template fornecido no Apêndice 1.

Antes de qualquer tratamento de Dados Pessoais, o Subcontratante deve verifcar que os Dados Pessoais tratados não envolvem um elevado risco para os direitos e liberdades das pessoas singulares. Se o Subcontratante, depois de ter verificado que o tratamento não está sujeito a uma Avaliação de Impacto sobre Proteção de Dados (AIPD) - Privacy Impact Assessment (PIA) - obrigatório de acordo com as situações listadas no Regulamento 1/2018 da CNPD, considera que pelo menos dois critérios das Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 adoptadas pelo Grupo de Trabalho do art. 29º para a Protecção de Dados (WP29) são correspondidos, a FI Group deve ser informada pelo Subcontratante da dúvida razoável quanto à necessidade de avaliação de impacto. Se a FI Group considerar que a PIA é necessária, o Subcontratante deve tomar o tempo necessário para ser parte disso.
O tratamento não deve começar até a PIA estar concluída.

Da mesma forma, se dados sensíveis no âmbito do Artigo 9 ou em conceção com condenações/infrações criminais tiverem de ser identificados, o Subcontratante compromete-se a notificar imediatamente a FI Group antes de iniciar a recolha de Dados Pessoais.
Também deve demonstrar que não há outra solução possível e certificar—se o mais rápido possível notificando a FI Group, no caso de uma Falha de Segurança ou Violação.

ARTIGO 5 – TRANSMISSÃO E USO DE DADOS

Sob o Acordo Contractual, o Responsável pelo Tratamento deve comunicar Dados Pessoais de qualquer tipo e em qualquer meio ao seu Subcontratante.

De acordo com o princípio de finalidade (propósito) só os dados estritamente necessários para a realização do Serviço devem ser recolhidos. Como tal, o Subcontratante deve responsabilizar-se, de acordo com o princípio de minimização de recolha de dados, a ser solicitado pela FI Group o mínimo de informação necessária e o seu uso apenas para o serviço. Assim, o Subcontratante não deve usar Dados pessoais para proveito próprio, principalmente para fins comerciais, de prospeção, marketing, estatística ou outros.

O Subcontratante garante que age a pedido de "instruções documentadas" do Responsável pelo Tratamento e deve imediatamente informar este último se alguma destas instruções constitui uma violação de uma obrigação legal ou regulamentar. Uma instrução do Responsável pelo Tratamento deve ser documentada pelo Subcontratante utilizando qualquer forma escrita.

Se um Subcontratante descobrir que os Dados Pessoais transmitidos não são ou deixarão de ser utilizados, deve responsabilizar-se, depois de notificar o Responsável pelo Tratamento, a aplicar o mesmo destino ao fornecido no Artigo 3, relativo ao período de retenção de Dados Pessoais no fim do Acordo Contractual.

ARTIGO 6 – INFORMAÇÃO E CONTROLO

A pedido da FI Group, o Subcontratante compromete-se a fornecer, no prazo de sete (7) dias úteis, um relatório detalhado sobre medidas de segurança técnicas e organizacionais aplicadas. Em caso de alteração do método de segurança, o Subcontratante deve fornecer à FI Group um relatório simplificado no mês seguinte à modificação.

De acordo com o RGPD, o Subcontratante compromete-se a manter um registo atualizado de Tratamento de Dados que deve ser disponibilizado à CNPD. O Processador de Dados concorda em fornecer à FI Group o seu Registo de Processamento de Dados no prazo de sete (7) dias úteis após pedido por escrito. Este atraso pode ser encurtado se o pedido vier de uma Terceira parte cujo atrasos impostos não são compatíveis com o atraso estipulado na Política.

No caso de séria dúvida sobre a veracidade destes elementos comunicados, a FI Group reserve-se no direito de questionar o seu Subcontratante pela comunicação de qualquer documento que permita garantir o nível de segurança em vigor.

Além disso, para garantir que as medidas técnicas e organizacionais implementadas pelo Subcontratante são suficientes, o Responsável pelo Tratamento reserva-se no direito de realizar auditorias dentro dos seus escritórios sem nunca exceder uma auditoria por ano civil.
O Responsável pelo Tratamento deve informar o Processador de Dados quinze (15) dias antes da auditoria.
O Subcontratante tem a possibilidade de adiar a auditoria por quinze (15) dias se a data não for adequada.
O Subcontratante deve comprometer-se a cooperar nestas auditorias e, em especial, comunicar toda a informação considerada necessária para a realização da mesma.
Especifica-se expressamente que um relatório de auditoria que não revele qualquer irregularidade é uma condição determinante para a continuação do Acordo Contractual.
No evento de incumprimento descrito no relatório da auditoria, o Subcontratante deve ser capaz de apresentar as ações corretivas no prazo de trinta (30) dias desde a submissão do relatório de auditoria. Se estas forem convincentes o suficiente para o Responsável pelo Tratamento, o acordo Contractual deve manter-se. Se ações corretivas forem consideradas insuficientes pelo Responsável pelo Tratamento, o acordo contractual deve ser terminado através de carta registada com aviso de receção sem outro formalismo.

ARTIGO 7 – APROVAÇÕES NECESSÁRIAS

1) Requisitos para Terceiros

No exercício dos seus Serviços, o Subcontratante deve abster-se de utilizar outros sub-processadores se, à data da assinatura do Acordo Contractual não estiver a trabalhar com nenhum Terceiro.

Se for necessário recorrer-lhes, o Subcontratante deve fornecer a lista de Terceiro(s) envolvidos e solicitar autorização escrita do Responsável pelo Tratamento, que reserve o direito de aceitar ou não. No evento de recusa pelo Responsável pelo Tratamento, o Subcontratante pode (i) propor outro Terceiro, (ii) ou propor novamente o Terceiro que foi inicialmente recusado pelo Responsável pelo Tratamento, ao colocar antes de quaisquer medidas corretivas solicitadas pelo Responsável pelo Tratamento. Se nenhuma destas possibilidades for aceite, o Subcontratante não terá recurso a este Terceiro.

Como exceção às condições acima referidas, se no momento da assinatura o Subcontratante informou o Responsável pelo Tratamento sobre o uso de Terceiros e forneceu uma lista dos Terceiros envolvidos, o acesso aos Dados Pessoais do Responsável pelo Tratamento é autorizado.
Assim, caso de uso de Terceiros sob as condições previamente mencionadas, o Subcontratante deve informá-los sobre a Política e comprometer-se a garantir que a respeitam, relembrando que o Subcontratante se mantém totalmente responsável perante o Responsável pelo Tratamento pelas consequências do incumprimento das obrigações incumbidas aos Terceiros.

No caso de modificação da lista, o Subcontratante compromete-se a notificar quaisquer mudanças ao Responsável pelo Tratamento que possa ocorrer com um (1) mês de avanço. Assim, a FI Group pode opor-se à divulgação dos Dados Pessoais a um novo Subcontratante. Em caso de omissão de um Subcontratante da lista, a FI Group reserve-se no direito de recorrer diretamente a este ultimo para lhe dar conhecimento do respeito das obrigações associadas ao fim do serviço.

2) Requisitos relativos ao processamento de dados pessoais relacionados com os direitos do Titular de Dados

O Subcontratante está proibido de qualquer reprodução e/ou qualquer transferência sem a autorização previa do seu Responsável pelo Tratamento.

Neste contexto, o Subcontratante abstém-se de dar acesso, corrigir, apagar, ou bloquear Dados Pessoais exceto com o consentimento expresso do Responsável pelo Tratamento.
Em caso de pedido de uma pessoa singular, depois de ter verificado previamente a identidade da pessoa em causa, o Subcontratante deve assegurar-se que transmite o pedido para acesso, correção, ou apagamento ao Responsável pelo Tratamento para que este possa enviar instruções necessárias para processar este pedido, no prazo de dois (2) dias úteis.

ARTIGO 8 – TROCAS DE SEGURANÇA

Para todas as questões gerais relacionadas com o processamento de Dados Pessoais, o Subcontratante e a FI Group podem recorrer aos contactos identificados no Apêndice 1.

Como parte do Serviço, o Subcontratante e o Responsável pelo Tratamento podem estabelecer simultaneamente, com a assinatura da Política pelo Subcontratante, uma lista de pessoas de contacto dentro do respetivo departamento a quem os Dados Pessoais podem transitar.

Em caso de alteração da lista, o Subcontratante e o Responsável pelo Tratamento devem informar-se um ao outro desta modificação por escrito. A parte informada deve reconhecer a receção desta informação.

ARTIGO 9 – MEDIDAS DE SEGURANÇA COBRADAS AO PROCESSADOR DE DADOS

O Subcontratante deve criar medidas técnicas e organizacionais para garantir a segurança adequada do Tratamento. Deve, pelo menos, fornecer:

- Bloqueio sistemático de equipamento informático que contenha dados pessoais deixados sem vigilância.

- A alteração recorrente de passwords para todas as pessoas que tenham acesso aos Dados Pessoais no desempenho do Serviço. Esta alteração deve acontecer dentro de um período de tempo, alinhado com a critica de Dados Pessoais.
- Um local de armazenamento com acesso Seguro assim que os dados pessoais são comunicados num suporte hardware (papel, USB, etc.).

Como exceção ao referido acima, o Subcontratante deve permanecer livre para implementar quaisquer medidas de segurança para que estas sejam pelo menos iguais às medidas referidas neste artigo.

O Subcontratante deve comprometer-se a respeitar e assegurar a confidencialidade dos Dados Pessoais dos seus colaboradores.

O Subcontratante deve comprometer-se a formar os seus colaboradores na obtenção de Dados Pessoais.

4. Transferência de Dados Pessoais para fora da UE

ARTIGO 10 – PRINCIPIO DA PROIBIÇÃO DE TRANSFERÊNCIA DE DADOS PESSOAIS PARA FORA DA UE

Por princípio, a transferência de Dados Pessoais para fora da UE não é permitida.

Como exceção, países beneficiários do acordo de Adequação segundo o procedimento referido no Artigo 45 da RGPD devem ser considerados como parte da UE e as transferências devem ter lugar sem autorização prévia. No entanto, no caso de mudanças que levem à anulação do acordo de Adequação, o Subcontratante deve usar o procedimento referido no Artigo 11 da Política.

ARTIGO 11 – EXCEPÇÕES PARA A TRANSFERÊNCIA DE DADOS PESSOAIS PARA FORA DA UE

Transferência de Dados Pessoais só deverá ser possível se acumular as seguintes condições:

- Um interesse dentro da execução do acordo contractual

- Um pedido expresso – através ou de o Apêndice, quando o assinar, ou através de uma atualização do mesmo

- A transferência deve ser protegida pelas medidas apropriadas, referidas no Artigo 46 da RGPD.

Na ausência de medidas adequadas, conforme estabelecido exaustivamente pelo artigo 46 do GDPR, o Subcontratante pode demonstrar que as obrigações do artigo 47 do GDPR são cumpridas, desde que a transferência não seja repetitiva e diga respeito a um número limitado de pessoas.

5. Informação e instruções em caso de falha de Segurança dos Dados Pessoais

ARTIGO 12 – FALHA DE SEGURANÇA DADOS PESSOAIS

Para antecipar as medidas implementadas em caso de Violação de Dados Pessoais, o Subcontratante deve comunicar à FI Group o método usado se o risco for realizado.

Este método deve ser comunicado no Relatório Detalhado e, se aplicável, o Relatório Simplificado que deve ser automaticamente devolvido em caso de Violação. Para apoiar esta informação, a FI Group deve ser capaz de avaliar a adaptabilidade e eficácia destas medidas.

No prazo de 24 horas após a Violação de Dados Pessoais, o Subcontratante deve comprometer-se a informar imediatamente o Responsável pelo Tratamento dos meios implementados através de um registo de Falha de Segurança que se mantém atualizado.
Em caso de identificação de um risco que pode afetar a segurança dos Dados Pessoais, o Subcontratante deve comprometer-se a notificar a FI Group no prazo de 72 horas. Está expressamente especificado que o Subcontratante não deve liberar-se de qualquer obrigação de alertar a FI Group, aproveitando um risco que não ocorreu ou um "baixo" nível de falha de segurança.

Assim que o risco tenha sido identificado, o Subcontratante deve comprometer-se a implementar medidas corretivas para garantir um nível mais eficiente de proteção do que inicialmente previsto em caso de falha da Segurança de Dados Pessoais.

5. Sanções e fim do Serviço

ARTIGO 13 – SANÇÕES

Em caso de incumprimento de uma das suas obrigações ao abrigo da Política, incluindo, mas não se limitando, ao incumprimento de um Subcontratante subsequente, resultando numa sanção financeira por parte da CNPD ou de quaisquer outras entidades jurídicas habilitadas a sancionar o Responsável pelo Tratamento, o Subcontratante compromete-se a reembolsar ao Responsável pelo Tratamento a quantia que não possa ser atribuída à inconsistência do Subcontratante.

No evento de ação, queixa, exigência, ou oposição de terceiros ligados a um incumprimento pelo Subcontratante para assumir a responsabilidade total e reembolsar os custos juntamente com prova ao Responsável pelo Tratamento.

A FI Group pode exigir o fim da relação com o Subcontratante por qualquer defeito de uma obrigação essencial e decisiva. Consequentemente, a terminação imediata e automática do acordo Contractual.

ARTIGO 14 – FIM DO SERVIÇO

O Subcontratante deve prometer respeitar as obrigações estabelecidas como no Acordo 3 e emitir um certificado de arquivo/destruição no primeiro pedido após um (1) mês a seguir ao fim do Serviço. A obrigação de confidencialidade retém todos os seus efeitos por um período ilimitado de tempo após o fim do Serviço.

Empresa:
Sr/Sra:
Menção escrita "bom para acordo"
Data, carimbo e assinatura