POLITICA PRIVACIDADE DADOS

DATA: 14/05/2018
VERSÃO: 1

ELABORADO POR: Carlos Monteiro Ribeiro

REVISTO POR: ----------

APROVADO POR: Gilson Membrive

1. CONTEXTO, QUESTÕES E DESAFIOS

A EMFILS está profundamente empenhada em proteger os Dados pessoais e a Privacidade.

A EMFILS trata dados pessoais relativos aos seus funcionários, clientes, parceiros, prestadores de serviços e fornecedores no curso das suas actividades quotidianas (gestão de pessoal, prospecção e gestão de soluções para clientes, etc.).

Os indivíduos estão cada vez mais conscientes dos dados que partilham e esperam um tratamento adequado e a protecção dos seus dados pessoais.

As entidades públicas estão cada vez mais conscientes destas temáticas. Estão-se a criar obrigações mais rigorosas para as empresas que processam dados pessoais e podem ser perseguidas através de sanções civis, penais e financeiras. Assim, a EMFILSe suas Entidades têm de cumprir com o Regulamento Europeu Nº 2016/679 de 27/04/2016, relativo à protecção de dados pessoais.

Consequentemente, a EMFILS encontra-se cada vez mais exposto aos riscos associados à inapropriada recolha, uso, alteração, comprometimento e até mesmo falsificação de dados pessoais internos ou externos.

Com base nos seus valores éticos em relação a dados pessoais e à privacidade e, ciente da importância das regras de protecção de dados e privacidade e dos riscos em caso de violação, a EMFILS compromete-se a proteger tais dados e privacidade e, consequentemente, a implementar a política definida neste documento.

2. ÂMBITO E OBJETIVOS

A Política está alinhada com o Código de Conduta de Proteção de Dados.

Os princípios da presente Política baseiam-se nas convenções internacionais listadas no Anexo 2. Em caso de qualquer conflito entre a Política e as convenções internacionais aplicáveis ou a regulamentações nacional aplicável à EMFILS, esta última terá precedência sobre estes princípios.

A Política de Privacidade de Dados da EMFILS aplica-se a todos os seus colaboradores e Clientes.

Esta Política será reforçada e aprofundada com o acréscimo progressivo de outros documentos (metodologias, procedimentos, boas práticas, sensibilização, etc.) que permitirão alcançar os objectivos definidos.

Os requisitos a seguir devem ser cumpridos antes da implementação efectiva de qualquer tratamento de dados pretendido e, portanto, devem ser levados em conta no planeamento de qualquer projecto que envolva o tratamento de dados pessoais. Uma vez implementado, o tratamento de dados deve sempre respeitar os princípios descritos nesta Política. Requisitos semelhantes também podem ser aplicados no caso de uma alteração das condições sob as quais o tratamento de dados é executado.

3. DEFINIÇÕES

DADOS PESSOAIS:

Informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, directa ou indirectamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via electrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular *(RGPD, art. 4º)*.

TRATAMENTO:

Uma operação ou um conjunto de operações efectuadas 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 *(RGPD, art. 4º).*

RESPONSÁVEL PELO TRATAMENTO:

A pessoa singular ou colectiva, 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 *(RGPD, art. 4º).*

CONSENTIMENTO:

Manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento *(RGPD, art. 4º).*

VIOLAÇÃO DE DADOS PESSOAIS:

Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento *(RGPD, art. 4º).*

4. GOVERNANÇA

Os objectivos e meios de protecção dos dados pessoais aqui descritos devem ser implementados ao nível da EMFILS.

A EMFILS deve garantir a conformidade com a Política de Privacidade de dados e com as leis aplicáveis à Protecção de Dados antes da implementação do tratamento de dados e durante toda a sua execução e operação.

A EMFILS poderá designar um Encarregado de Protecção de Dados de forma a garantir a conformidade com a legislação nacional.

O Encarregado de Protecção de Dados deve receber os recursos e tempo necessários para cumprir a missão que lhe foi atribuída. Uma vez que está incumbido de aplicar a presente Política e assegurar o cumprimento do Regulamento Europeu.

O Encarregado de Protecção de Dados:

- Está sujeito aos requisitos de sigilo profissional e acesso directo aos dados (ou seja, não pode ser negado o acesso aos dados);
- É independente e reporta ao mais alto nível da EMFILS;
- Está obrigado a notificar a Autoridade de Protecção de Dados de quaisquer incidentes (violação de dados) dentro de 72 horas e, se necessário, informar os titulares dos dados afectados;
- Está obrigado a realizar ou organizar a execução de auditorias e inspeções.

4.1. Outras Partes Interessadas

Os responsáveis pela segurança cibernética e da informação (CISOs) devem dar o seu suporte e conhecimento na área da privacidade de dados, quer para tratamento de dados alojados internamente quer em terceiros. As principais funções do CISO nesta área são as seguintes:

- auxiliar o Encarregado Protecção de Dados na classificação de dados pessoais e na implementação de projectos IT;
- aconselhar na selecção de funções e sistemas de privacidade de dados;
- ser o ponto de contacto para todos os pedidos relacionados com os aspectos de confidencialidade e segurança de um tratamento de dados em produção.

Os gestores de projecto que actuam em nome do responsável de tratamento de dados e que tratem dados pessoais, devem garantir que a privacidade de dados é mantida durante todo o projecto.

As Direcção Jurídica e de Recursos Humanos devem oferecer conselhos e informações com relação à legislação e jurisprudência aplicáveis.

Todos os colaboradores (quer permanentes quer temporários) são responsáveis, ao seu nível, pelos dados pessoais que acedem e tratam.

Todos os colaboradores que implementem uma aplicação que trata dados pessoais deve primeiro informar o Encarregado Protecção de Dados, pois o tratamento de dados pode exigir notificação prévia a uma Autoridade de Protecção de Dados ou consentimento dos titulares.

Qualquer terceiro, incluindo responsáveis de tratamento de dados, fornecendo serviços em nome da EMFILS, deve estar ciente dos princípios desta Política com relação aos dados pessoais que acedem e tratam.

4.2. Medidas de Segurança

A EMFILS tem implementadas medidas de segurança logicas, físicas, organizativas e de segurança adequadas, necessárias e suficientes para proteger os dados contra a destruição, perda, alteração, difusão, acesso não autorizado ou qualquer outra forma de tratamento acidental ou ilícito.

5. OS PRINCÍPIOS DA PROTECÇÃO DE DADOS

Os princípios de protecção apresentados seguidamente aplicam-se a todas as Entidades EMFILS, a menos que a legislação nacional seja contrária ou mais rigorosa.

Princípio	***Requisitos***
Finalidade explicita, licita, leal e transparente	Os dados pessoais devem ser tratados para **fins específicos, explícitos e legais**. A informação enviada ao titular dos dados deve ser **concisa, facilmente acessível e compreensível.**
Relevância, minimização e proporcionalidade	A recolha de dados pessoais deve ser **adequada, pertinente, exacta e actualizada**, se necessário, e **relevante e limitada ao estritamente necessário.**
Limitação da conservação	O período de conservação dos dados pessoais tratados deve ser definido de acordo com o objectivo da recolha e com a legislação em vigor. Os titulares dos dados devem ser notificados do período de conservação, ou, se isso não for possível, os critérios usados para determiná-lo. Após o tempo de conservação os dados pessoais devem ser apagados ou anonimizados.
Dados Sensíveis	Os dados sensíveis apenas podem ser tratados com o consentimento explícito do titular dos dados ou sob circunstâncias expressamente autorizadas pela legislação em vigor. Os dados sensíveis incluem também a associação a sindicatos e dados genéticos ou biométricos para a identificação única de um indivíduo.
Integridade e confidencialidade	Devem ser tomadas todas as medidas de protecção apropriadas para garantir a **integridade e a confidencialidade** dos dados pessoais. Para garantir a integridade e confidencialidade dos dados tratados, devem ser tomadas medidas como o pseudonimização, anonimização e encriptação.
Transferências Internacionais	Quando se transferir dados pessoais para entidades fora da UE, deve-se garantir que os países para onde os dados são transferidos oferecem, no mínimo, o nível de protecção descrito nesta Política e os requisitos específicos da regulamentação da UE.
Abertura e respeito pelos direitos dos indivíduos	Políticas transparentes devem ser implementadas com relação aos direitos dos titulares dos dados, tais como: **direito à transparência, à informação, à notificação, ao acesso, à rectificação, ao apagamento, à limitação do tratamento, à portabilidade, à oposição e à não sujeitação de decisões automatizadas.**
Obrigações do Responsável pelo Tratamento dos Dados	Qualquer Entidade que subcontratar um tratamento de dados a um processador de dados, permanece responsável pela protecção dos dados pessoais. As entidades devem garantir que os dados são tratados de acordo com os princípios de protecção da Política de Privacidade de Dados da EMFILS e da regulamentação da UE. Deve ser estabelecido um contracto ou acordo prevendo que as obrigações do responsável pelo tratamento cumpre as regras de protecção de dados pessoais, incluindo medidas de

confidencialidade e integridade.

6. RECURSOS

Os seguintes recursos devem ser implementados para atingir os objectivos desta Política.

Recurso	***Objectivo***
Sensibilização e formação	Todos os colaboradores devem estar cientes das questões que envolvem a privacidade dos dados. Campanhas de sensibilização global são realizadas ao nível do Grupo EMFILS; As acções locais são realizadas para complementar as campanhas da EMFILS.
Avaliações e Auditorias	As avaliações de conformidade internas com a presente Política e a com a regulamentação de protecção de dados devem ser realizadas regularmente pelo Encarregado de Protecção dos Dados ou pelo departamento de auditoria interna da EMFILS. Como parte dessas avaliações, o acesso a processos e dados, bem como, por exemplo, a medidas de confidencialidade e integridade e os períodos de conservação devem ser revistos e controlados.
Mapeamento das Operações de Tratamento de dados	Em relação ao princípio da abertura e para facilitar o exercício do direito de acesso dos titulares dos dados, a EMFILS mapea todas as operações de tratamento de dados. Além de oferecer uma visão geral abrangente, este mapeamento permitirá que o tratamento de dados seja controlado e racionalizado, e o registro facilitará o tratamento pela responsável pelo tratamento e o acesso pelo titular dos dados.
Gestão de Incidentes	Qualquer colaborador que tenha conhecimento de um uso inadequado de dados pessoais deverá entrar em contacto com a pessoa responsável pela proteção de dados (protecao.dados@EMFILS.com). A pesso responsável pela Protecção de Dados e ou o Responsável pelo Tratamento terá de notificar a violação de dados dentro de 72h à Autoridade de protecção de Dados e ao Responsável de Ética. Quando necessário, deverá também informar os titulares dos dados afectados.
Acordos Escritos	Nos casos de serviços que impliquem o tratamento de dados pessoais (por exemplo: medicina do trabalho, seguradoras e acesso a instalações dos clientes), deve ser estabelecido um acordo por escrito entre as partes envolvidas (EMFILS, seus clientes ou parceiros). Em qualquer circunstância, a recolha e o uso de dados pessoais deve estar em conformidade com as leis em vigor, o Código de Conduta da EMFILS e a presente Política.

7. RESPONSABILIZAÇÃO

A responsabilização é o princípio fundador do regulamento europeu. Envolve maior responsabilidade do responsável pelo tratamento de dados.

Envolve a capacidade da EMFILS demonstrar, a qualquer momento, a sua conformidade com os princípios de protecção de dados e a eficácia das medidas tomadas. As ferramentas de conformidade da responsabilidade são:

- registro de tratamento de dados;
- a implementação de procedimentos que levem em conta: a privacidade por design, privacidade por padrão, avaliação do impacto na privacidade;
- certificações e códigos de conduta em relação à protecção de dados no que diz respeito às actividades da EMFILS.

A implementação da presente Política é um dos componentes essenciais da responsabilização para alcançar a conformidade com o Regulamento Europeu.

Acesso à Declaração Universal dos Direitos Humanos:
http://www.un.org/en/documents/udhr/

O Artigo 12 da Declaração Universal dos Direitos Humanos das Nações Unidas declara*: Ninguém será submetido a interferências arbitrárias na sua privacidade…*
O Artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos (Escritório do Alto Comissariado para os Direitos Humanos) declara: *Ninguém será submetido a interferências arbitrárias ou ilegais na sua privacidade…*

Acesso à Convenção Europeia dos Direitos Humanos:
http://www.echr.coe.int/Documents/Convention_ENG.pdf

O artigo 8.º da Carta dos Direitos Fundamentais da União Europeia estabelece:

1. *Toda pessoa tem direito à protecção de Dados Pessoais relativos a ela.*
2. *Tais dados devem ser tratados de forma justa para fins específicos e com base no consentimento da pessoa em causa ou outra base legítima estabelecida por lei. Todos têm o direito de acesso a dados recolhidos sobre ele ou ela e o direito de rectificá-lo. …*

Acesso ao Pacto Internacional sobre Direitos Civis e Políticos:
http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Directrizes da OCDE para a Protecção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais (1980/2013)

Acesso às Orientações:
http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Lista de Membros (34 à data da publicação) :
http://www.oecd.org/about/membersandpartners/

Directiva 95/46 / CE relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Acesso à Directiva :
http://ec.europa.eu/justice/data-protection/index_en.htm

Acesso aos Estados-Membros (28 à data da publicação):
http://europa.eu/about-eu/countries/index_en.htm

Regulamento UE 2016/679 de 27/04/2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (aplicável a partir de 25 de maio de 2018).
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

APEC Privacy Framework (2005)

Acesso ao Quadro de Privacidade:
http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx

Lista dos membros da APEC: (21 na data da publicação)
http://www.apec.org/about-us/about-apec/member-economies.aspx

ANEXO 1 – DOCUMENTOS DE REFERÊNCIA

GAPP – Generally Accepted Privacy Principles – Desenvolvido pela AICPA & CICA (agosto de 2009))

Acesso à GAPP :
http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/pages/default.aspx

AICPA : American Institute of Certified Public Accountants
http://www.aicpa.org/Pages/default.aspx

CICA : Canadian Institute of Chartered Accountants
http://www.cica.ca/index.aspx

Resolução de Madri sobre Proposta Conjunta para um Projeto de Norma Internacional sobre a Proteção de Dados Pessoais e Privacidade (11/9/2009).

Acesso ao comunicado de imprensa:
http://www.gov.im/lib/docs/odps/madridresolutionpressreleasenov0.pdf

Acesso ao Projeto de Norma Internacional:
http://www.gov.im/lib/docs/odps/madridresolutionnov09.pdf