Nota inicial: Este documento serve de apoio e consulta ao responsável pelo tratamento de dados e ao DPO para a criação da Avaliação de Impacto sobre a Proteção de Dados.

**AIPD – Avaliação do Impacto da Proteção de Dados (ou *PIA* – *Privacy Impact Assessment*)**

O presente documento descreve a AIPD – Avaliação do Impacto da Proteção de Dados, de acordo com o Regulamento Geral da Proteção de Dados. Com o objetivo de elucidar todos aqueles que desempenham funções de tratamento dos dados, encontrará respostas às principais questões que surgem quando se fala da Avaliação do Impacto da Proteção de Dados.

# **O que é?**

É uma avaliação de impacto do tratamento de dados pessoais. Esta avaliação deve ser realizada sempre que há lugar a tratamento de dados que apresentem riscos de violação de privacidade, quer pela sua natureza, quer no âmbito das atividades desenvolvidas. Esta avaliação prévia permite que as entidades, ao identificarem problemas na fase inicial, reduzam os custos associados ao incumprimento do Regulamento Geral da Proteção de Dados.

# **Quem deve realizar a AIPD?**

Todas as empresas que efetuam o tratamento de dados pessoais que podem resultar num risco elevado aos direitos do titular dos dados. Esta avaliação não é da responsabilidade do EPD (Encarregado pela Proteção de Dados), mas sim do responsável pelo tratamento dos dados. No entanto, o EPD pode desempenhar um papel muito importante e útil, prestando assistência ao responsável pelo tratamento. Ao abrigo do artigo 35º, nº2, o responsável pelo tratamento deve “solicita[r] o parecer” do encarregado pela proteção de dados e, de acordo com o artigo 39.º, n.º 1, alínea c), o EPD deve “prestar aconselhamento, quando tal lhe for solicitado, no que respeita à AIPD, e controlar a sua realização nos termos do artigo 35.º”.

# **Quando deve ser realizada?**

Esta avaliação de impacto deve ser realizada antes de dar início ao tratamento dos dados pessoais.

# **Situações em que a mesma é obrigatória:**

a)Sempre que existe uma avaliação sistemática e extensiva de aspetos pessoais relacionados com cidadãos, baseada em processamento automatizado, incluindo definição de perfis, que poderão afetar significativamente a pessoa. (Ex.: Instituições financeiras que aprovam empréstimos de forma automatizada, empresas de marketing *online* e motores de busca com alvos de marketing).

b) Sempre que existe tratamento de dados pessoais sensíveis em larga escala e dados pessoais relativos a convicções criminais. (Ex.: Companhias de seguros, fornecedores de cuidados de saúde).

c) Monitorização sistemática de áreas públicas em larga escala (Ex.: Autoridades locais que utilizem circuitos fechados de televisão em áreas públicas).

# **Consulta prévia**

Enquanto responsável pelo tratamento dos dados, deverá consultar a autoridade supervisora sobre a possibilidade de o tratamento dos dados resultar num elevado risco à segurança dos dados pessoais. Sempre que esta considerar que o tratamento dos dados não cumpre o RGPD, deverá fornecer aconselhamento por escrito ao responsável pelo tratamento dos dados. Como parte do processo de consulta, a autoridade supervisora solicitará:

1) As responsabilidades do responsável pelo tratamento dos dados;

2) Finalidades e meios de tratamento dos dados;

3) Medidas de segurança utilizadas para proteger os dados pessoais;

4) Informações de contacto do EPD (Encarregado da Proteção de Dados);

5) AIPD (Avaliação de Impacto da Proteção dos Dados).

# **Como é realizado o processo da AIPD?**

Um compromisso de AIPD pode variar dependendo da natureza e complexidade das operações de tratamento. O processo envolve normalmente vários intervenientes cruciais dentro da empresa e é supervisionado por um “responsável interno” – o atual DPO ou EPD (Encarregado da Proteção de Dados) ou alguém que desempenha esta função a meio-termo. Antes de se dar início à avaliação de impacto de risco, devem ser tidas em conta as seguintes condições e medidas, aquando da determinação de conformidade e prática do processo:

1) Sempre que o tratamento é suscetível de atribuir risco aos dados

2) Envolvimento do DPO

3) Avaliação sistemática do tratamento proposto

4) Identificação do risco

5) Resumo das medidas a tomar para reduzir esses riscos

6) Resumo de estruturas e medidas planeadas para alcançar o consentimento

7) Sempre que é identificado o risco substancial, o responsável pelo tratamento dos dados deve confirmar com a autoridade de controlo.

De modo a estabelecer:

1. Proveniência dos dados
2. Meio de tratamento envolvido
3. Localização do tratamento
4. Intervenientes relevantes
5. Processo de eliminação/anonimização

É levado a cabo um processo de 6 passos:

1. Criação de uma listagem completa de todos os intervenientes, entidades e sistemas relevantes na empresa.
2. Criação de uma listagem completa de processos de gestão de dados.
3. Definição do fluxo de dados que entram e saem da empresa, tendo em conta os processos referidos no ponto anterior.
4. Para cada processo identificado no ponto anterior, o tratamento é categorizado de acordo com a atual e futura legislação sobre a Proteção de Dados, áreas de consideração e avaliação de potencial risco.
5. Criar um registo de risco[[1]](#footnote-1) em paralelo com o ponto anterior de modo a medir a probabilidade e gravidade do risco.
6. Formalizar um plano de implementação, ou seja, geração de um relatório por parte da AIPD que identifica as áreas de elevado risco e fornece recomendações específicas de como resolver cada risco. Para além disso, sempre que possível, são feitas recomendações práticas de como é que a empresa poderá melhorar a conformidade de acordo com a legislação de proteção de dados nacional.

Para o ajudar a compreender melhor o processo da Avaliação do Impacto da Proteção de Dados, abaixo encontra um gráfico com os pontos principais que constituem o mesmo.

1. O registo de risco é produzido pela AIPD e inclui: detalhes específicos sobre o risco, recomendações, próximos passos, ações até à data e a avaliação do risco em si. [↑](#footnote-ref-1)