



17/PT

WP 248 rev.01

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

Adotadas em 4 de abril de 2017

Revistas e adotadas pela última vez em 4 de outubro de 2017

Este grupo de trabalho foi instituído ao abrigo do artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições encontram-se descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

Os serviços de secretariado são prestados pela Direção C (Direitos Fundamentais e Cidadania da União) da Comissão Europeia, Direção-Geral de Justiça, B-1049 Bruxelas, Bélgica, Gabinete n.º MO-59 03/075.

Sítio web: http://ec.europa.eu/justice/data-protection/index_en.htm

O GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS

instituído pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,

tendo em conta os artigos 29.º e 30.º da referida diretiva,

tendo em conta o seu regulamento interno,

ADOTOU AS PRESENTES ORIENTAÇÕES:

Índice

I. INTRODUÇÃO	4
II. ÂMBITO DE APLICAÇÃO DAS ORIENTAÇÕES	5
III. AIPD: UMA EXPLICAÇÃO DO REGULAMENTO	7
A. O QUE ABRANGE UMA AIPD? UMA ÚNICA OPERAÇÃO DE TRATAMENTO OU UM CONJUNTO DE OPERAÇÕES DE TRATAMENTO SEMELHANTES.	8
B. QUAIS SÃO AS OPERAÇÕES DE TRATAMENTO QUE ESTÃO SUJEITAS A UMA AIPD? PARA ALÉM DAS EXCEÇÕES, QUANDO SÃO «SUSCETÍVEIS DE IMPLICAR UM ELEVADO RISCO».	9
a) Quando é que uma AIPD é obrigatória? Quando o tratamento for «suscetível de implicar um risco elevado».	9
b) Quando é que uma AIPD não é obrigatória? Quando o tratamento não for «suscetível de implicar um elevado risco», quando já existir uma AIPD semelhante, quando tiver sido autorizado antes de maio de 2018, quando tiver um fundamento jurídico ou quando fizer parte de uma lista de operações de tratamento para as quais não seja necessária uma AIPD.	15
C. E RELATIVAMENTE ÀS OPERAÇÕES DE TRATAMENTO JÁ EXISTENTES? AS AIPD SÃO OBRIGATÓRIAS NALGUMAS CIRCUNSTÂNCIAS.	15
D. COMO REALIZAR UMA AIPD?	16
a) Em que altura deve ser realizada uma AIPD? Antes de se iniciar o tratamento.....	16
b) Quem está obrigado a realizar uma AIPD? O responsável pelo tratamento, com o encarregado do tratamento dos dados e os subcontratantes.....	17
c) Qual é a metodologia para realizar uma AIPD? Existem metodologias diferentes, mas os critérios são comuns.	18
d) Existe uma obrigação de publicar a AIPD? Não, mas a publicação de um resumo pode fomentar a confiança, e a AIPD completa deve ser comunicada à autoridade de controlo em caso de consulta prévia ou se tal for solicitado pela autoridade de proteção de dados.	21
E. QUANDO DEVE A AUTORIDADE DE CONTROLO SER CONSULTADA? QUANDO OS RISCOS RESIDUAIS SÃO ELEVADOS.	21
IV. CONCLUSÕES E RECOMENDAÇÕES.....	22
ANEXO 1 — EXEMPLOS DE QUADROS EXISTENTES NA UE EM MATÉRIA DE AIPD	24
ANEXO 2 — CRITÉRIOS PARA UMA AIPD ACEITÁVEL.....	26

I. Introdução

O Regulamento 2016/679¹ (RGPD) é aplicável a partir de 25 de maio de 2018. O artigo 35.º do RGPD introduz o conceito de Avaliação de Impacto sobre a Proteção de Dados (AIPD²), tal como a Diretiva 2016/680³.

Uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais⁴ avaliando-os e determinando as medidas necessárias para fazer face a esses riscos. As AIPD são instrumentos importantes em matéria de responsabilização, uma vez que ajudam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o regulamento (ver também artigo 24.º)⁵. Por outras palavras, **uma AIPD é um processo que visa estabelecer e demonstrar conformidade.**

¹ Regulamento (UE) n.º 2016/679 do Parlamento Europeu 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

² A expressão «Avaliação de Impacto na Privacidade» (AIP) é frequentemente utilizada noutros contextos como referência ao mesmo conceito.

³ O artigo 27.º da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, também refere que é necessária uma avaliação de impacto na privacidade «[c]aso um tipo de tratamento [...] seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares».

⁴ O RGPD não define formalmente o conceito de uma AIPD propriamente dita, mas

- o seu conteúdo mínimo encontra-se especificado no artigo 35.º, n.º 7, da seguinte forma:
 - o «a) *Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;*
 - o b) *Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;*
 - o c) *Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.º 1; e*
 - o d) *As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa».*
- qual o seu sentido e para que serve são aspetos que se encontram clarificados no considerando 84 da seguinte forma: «A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco».

⁵ Ver igualmente o considerando 84: «Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento».

Nos termos do RGPD, a não conformidade com os requisitos de uma AIPD pode conduzir à imposição de coimas pela autoridade de controlo competente. Não realizar uma AIPD quando o tratamento está sujeito a uma AIPD (artigo 35.º, n.º 1 e n.ºs 3 a 4), realizar uma AIPD de forma incorreta (artigo 35.º, n.º 2 e n.ºs 7 a 9) ou não consultar a autoridade de controlo competente quando necessário (artigo 36.º, n.º 3, alínea e)) pode resultar numa coima administrativa até 10 milhões de euros ou, no caso de uma empresa, até 2 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

II. Âmbito de aplicação das orientações

As presentes orientações têm em conta:

- a declaração do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados 14/EN WP 218⁶;
- as orientações do Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/EN WP 243⁷;
- o parecer do Grupo de Trabalho do Artigo 29.º sobre a limitação das finalidades 13/EN WP 203⁸;
- as normas internacionais⁹.

Em consonância com a abordagem baseada no risco incorporada no RGPD, não é obrigatório realizar uma AIPD para todas as operações de tratamento. Só existe obrigação de realizar uma AIPD quando o tratamento for «*suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*» (artigo 35.º, n.º 1). Por forma a assegurar uma interpretação coerente das circunstâncias em que é obrigatório realizar uma AIPD (artigo 35.º, n.º 3), as presentes orientações visam antes de mais clarificar esta noção e fornecer critérios para as listas a adotar pelas autoridades responsáveis pela proteção de dados nos termos do artigo 35.º, n.º 4.

De acordo com o artigo 70.º, n.º 1, alínea e), o Comité Europeu para a Proteção de Dados (CEPD) está habilitado para emitir diretrizes, recomendações e melhores práticas por forma a incentivar uma aplicação coerente do RGPD. O presente documento tem como finalidade antecipar esse trabalho futuro do CEPD e, por conseguinte, clarificar as disposições pertinentes do RGPD com vista a ajudar os responsáveis pelo tratamento a cumprir a lei e proporcionar certeza jurídica aos responsáveis pelo tratamento que são obrigados a realizar uma AIPD.

⁶ Declaração 14/EN WP 218 do Grupo de Trabalho do Artigo 29.º sobre o papel de uma abordagem baseada no risco em relação aos quadros jurídicos em matéria de proteção de dados, adotada em 30 de maio de 2014.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

⁷ Orientações do Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/EN WP 243, adotadas em 13 de dezembro de 2016.

http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

⁸ Parecer 03/2013 do Grupo de Trabalho do Artigo 29.º sobre a limitação das finalidades 13/EN WP 203, adotado em 2 de abril de 2013.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

⁹ Por exemplo, a norma ISO 31000:2009, *Gestão do risco — Princípios e linhas de orientação*, Organização Internacional de Normalização (ISO); ISO/IEC 29134 (projeto), *Information technology – Security techniques – Privacy impact assessment – Guidelines* [Tecnologia da Informação – Técnicas de segurança – Avaliação de impacto na privacidade – Orientações], Organização Internacional de Normalização (ISO).

As presentes orientações procuram igualmente promover o desenvolvimento de:

- uma lista comum dentro da União Europeia de operações de tratamento em relação às quais é obrigatório realizar uma AIPD (artigo 35.º, n.º 4);
- uma lista comum dentro da União Europeia de operações de tratamento em relação às quais não é necessário realizar uma AIPD (artigo 35.º, n.º 5);
- critérios comuns relativos à metodologia a utilizar quando se realiza uma AIPD (artigo 35.º, n.º 5);
- critérios comuns que especifiquem quando é que a autoridade de controlo deve ser consultada (artigo 36.º, n.º 1);
- recomendações que, sempre que possível, tirem partido da experiência adquirida nos Estados-Membros da UE.

III. AIPD: uma explicação do regulamento

O RGPD exige que os responsáveis pelo tratamento apliquem medidas adequadas para assegurar e comprovar a conformidade com o RGPD, tendo em conta, entre outros, «os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis» (artigo 24.º, n.º 1). A obrigação que recai sobre os responsáveis pelo tratamento de realizarem uma AIPD em determinadas circunstâncias não deve ser entendida no contexto da sua obrigação geral de fazer uma gestão adequada dos riscos¹⁰ decorrentes do tratamento de dados pessoais.

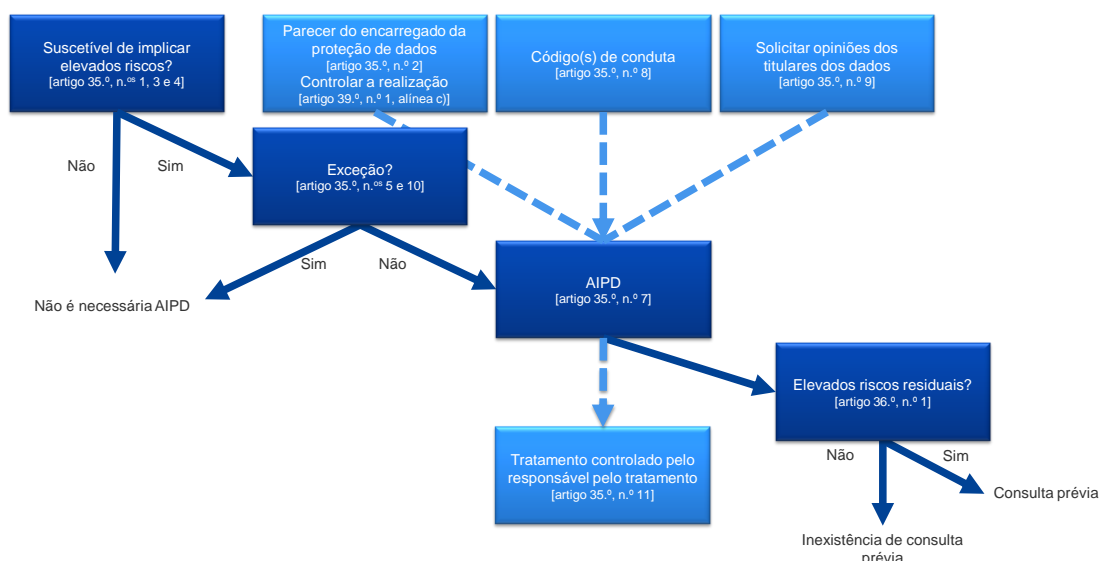
Um «risco» é um cenário que descreve um acontecimento e as respetivas consequências, estimado em termos de gravidade e probabilidade. Por outro lado, a «gestão do risco» pode ser definida como as atividades coordenadas que visam direcionar e controlar uma organização no que toca ao risco.

O artigo 35.º faz referência a um tratamento suscetível de implicar um elevado risco «para os direitos e liberdades das pessoas singulares». Como consta da declaração do Grupo de Trabalho do Artigo 29.º sobre o papel de uma abordagem baseada no risco em relação aos quadros jurídicos em matéria de proteção de dados, a referência aos «direitos e liberdades» dos titulares dos dados diz sobretudo respeito aos direitos de proteção dos dados e privacidade, mas também envolve outros direitos fundamentais como a liberdade de expressão, a liberdade de pensamento, a liberdade de circulação, a proibição de discriminação, o direito à liberdade, consciência e religião.

Em consonância com a abordagem baseada no risco incorporada no RGPD, não é obrigatório realizar uma AIPD para todas as operações de tratamento. Em vez disso, só existe obrigação de realizar uma AIPD quando um tipo de tratamento for «suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares» (artigo 35.º, n.º 1). Contudo, o simples facto de as condições que conduzem à obrigação de realizar uma AIPD não terem sido satisfeitas não diminui a obrigação geral que os responsáveis pelo tratamento têm de aplicar medidas que visem gerir adequadamente os riscos para os direitos e as liberdades dos titulares dos dados. Na prática, tal significa que os responsáveis pelo tratamento devem avaliar continuamente os riscos criados pelas suas atividades de tratamento por forma a identificarem quando um certo tipo de tratamento é «suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares».

¹⁰ Importa salientar que, por forma a gerir os riscos para os direitos e liberdades das pessoas singulares, os riscos têm de ser identificados, analisados, estimados, avaliados, tratados (p. ex. atenuados) e revistos regularmente. Os responsáveis pelo tratamento não podem fugir à sua responsabilidade, cobrindo os riscos com apólices de seguros.

A figura seguinte ilustra os princípios básicos relacionados com a AIPD no RGPD:



CNIL.

A. O que abrange uma AIPD? Uma única operação de tratamento ou um conjunto de operações de tratamento semelhantes.

Uma AIPD pode dizer respeito a uma única operação de tratamento de dados. Contudo, o artigo 35.º, n.º 1, estabelece que «[s]e um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação». O considerando 92 acrescenta que «[e]m certas circunstâncias pode ser razoável e económico alargar a avaliação de impacto sobre a proteção de dados para além de um projeto único, por exemplo se as autoridades ou organismos públicos pretenderem criar uma aplicação ou uma plataforma de tratamento comum, ou se vários responsáveis pelo tratamento planearem criar uma aplicação ou um ambiente de tratamento comum em todo um setor ou segmento profissional, ou uma atividade horizontal amplamente utilizada».

Uma única AIPD pode ser utilizada para avaliar múltiplas operações de tratamento que sejam semelhantes em termos de natureza, âmbito, contexto, finalidade e riscos. Na verdade, as AIPD visam estudar sistematicamente novas situações que possam ser suscetíveis de implicar riscos elevados para os direitos e as liberdades das pessoas singulares, não havendo necessidade de realizar uma AIPD para os casos que já foram estudados (ou seja, operações de tratamento realizadas num contexto específico e com uma finalidade específica). Pode acontecer que uma tecnologia semelhante seja utilizada para recolher os mesmos tipos de dados para os mesmos fins. Por exemplo, um grupo de autoridades municipais, em que cada uma dessas autoridades esteja a instalar um sistema de televisão em circuito fechado (CCTV) semelhante, pode realizar uma única AIPD que abranja o tratamento por parte destes responsáveis pelo tratamento independentes, ou então um operador ferroviário (responsável único) pode abranger a vigilância vídeo em todas as suas estações ferroviárias com uma única AIPD. Pode também ser aplicável a operações de tratamento semelhantes aplicadas por vários responsáveis pelo tratamento de dados. Nestes casos, deve ser partilhada ou disponibilizada ao público uma AIPD de referência, devem ser adotadas as medidas descritas na AIPD e deve ser fornecida uma justificação para a realização de uma única AIPD.

Quando a operação de tratamento envolve responsáveis conjuntos pelo tratamento, estes devem definir pormenorizadamente as respetivas obrigações. A sua AIPD deve definir qual das partes é responsável pelas várias medidas concebidas para dar resposta aos riscos e proteger os direitos e as liberdades dos titulares dos dados. Cada responsável pelo tratamento de dados deve exprimir as suas necessidades e partilhar informações úteis sem comprometer segredos (p. ex.: proteção de segredos comerciais, propriedade intelectual, informações empresariais confidenciais) ou revelar vulnerabilidades.

Uma AIPD também pode ser útil para avaliar o impacto na proteção de dados de um produto tecnológico, por exemplo, um equipamento ou um programa informático, sempre que este seja suscetível de ser utilizado por diferentes responsáveis pelo tratamento de dados para realizar diferentes operações de tratamento. É claro que o responsável pelo tratamento de dados que lança o produto continua obrigado a realizar a sua própria AIPD em relação à implementação específica, mas esta pode basear-se em informações de uma AIPD preparada pelo fornecedor do produto, se adequado. Um exemplo pode ser a relação entre os fabricantes de contadores inteligentes e as empresas de serviços públicos. Cada fornecedor ou subcontratante do produto deve partilhar informações úteis sem comprometer segredos e sem criar riscos de segurança divulgando vulnerabilidades.

B. Quais são as operações de tratamento que estão sujeitas a uma AIPD? Para além das exceções, quando são «suscetíveis de implicar um elevado risco».

Esta secção indica quando é que uma AIPD é obrigatória e quando é que não é necessário realizar uma AIPD.

Salvo se a operação de tratamento constituir uma exceção (III.B.a), terá de ser realizada uma AIPD quando uma operação de tratamento for «suscetível de implicar um elevado risco» (III.B.b).

a) Quando é que uma AIPD é obrigatória? Quando o tratamento for «*suscetível de implicar um risco elevado*».

O RGPD não exige a realização de uma AIPD para todas as operações de tratamento que possam implicar riscos para os direitos e as liberdades das pessoas singulares. A realização de uma AIPD é obrigatória somente quando o tratamento for «*suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*» (artigo 35.º, n.º 1, ilustrado pelo artigo 35.º, n.º 3, e complementado pelo artigo 35.º, n.º 4). É particularmente importante quando se introduz uma nova tecnologia de tratamento de dados¹¹.

Nos casos em que não é claro se a realização de uma AIPD é necessária, o Grupo de Trabalho do Artigo 29.º recomenda que, ainda assim, seja realizada uma AIPD, uma vez que uma AIPD é um instrumento útil para ajudar os responsáveis pelo tratamento a cumprir a legislação relativa à proteção de dados.

Ainda que possa ser necessário realizar uma AIPD noutras circunstâncias, o artigo 35.º, n.º 3, prevê alguns exemplos de quando é que uma operação de tratamento é «*suscetível de implicar elevados riscos*»:

- «a) *Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com*

¹¹ Para mais exemplos, ver os considerandos 89 e 91 e o artigo 35.º, n.ºs 1 e 3.

*base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar*¹²;

- b) *Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º*¹³; ou
- c) *Controlo sistemático de zonas acessíveis ao público em grande escala*».

Tal como se depreende da utilização da expressão «nomeadamente em caso de» na parte introdutória do artigo 35.º, n.º 3, do RGPD, a lista apresentada não é exaustiva. Podem existir operações de tratamento de «elevado risco» que não estejam incluídas nesta lista, mas que, ainda assim, impliquem riscos elevados. Estas operações de tratamento também devem estar sujeitas a AIPD. Por esta razão, os critérios desenvolvidos abaixo, por vezes, vão além de uma simples explicação acerca daquilo que deve ser entendido através dos três exemplos apresentados no artigo 35.º, n.º 3, do RGPD.

Com vista a fornecer um conjunto mais concreto de operações de tratamento que exigem uma AIPD devido ao elevado risco inerente, tendo em conta os elementos específicos dos artigos 35.º, n.º 1, e 35.º, n.º 3, alíneas a) a c), a lista a adotar a nível nacional nos termos do artigo 35.º, n.º 4, e dos considerandos 71, 75 e 91, e outras referências no RGPD a operações de tratamento «suscetível de implicar um elevado risco»¹⁴, devem ser considerados os seguintes nove critérios.

1. Avaliação ou classificação, incluindo definição de perfis e previsão, em especial de «*aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados*» (considerandos 71 e 91). Os exemplos deste critério podem incluir: uma instituição financeira que faça um controlo seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário ou a partir de uma base de dados de combate ao branqueamento de capitais e ao financiamento do terrorismo ou de combate à fraude; uma empresa de biotecnologia que ofereça testes genéticos diretamente aos seus clientes por forma a avaliar e prever riscos de doença ou para a saúde; ou uma empresa de desenvolva perfis comportamentais ou publicitários baseados na utilização ou navegação no seu sítio web.
2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar: tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza «*efeitos jurídicos relativamente à pessoa singular*» ou que «a afetem significativamente de forma similar» (artigo 35.º, n.º 3, alínea a)). Por exemplo, o tratamento pode implicar a exclusão ou a discriminação de indivíduos. O tratamento que produza poucos ou nenhuns efeitos relativamente aos indivíduos não satisfaz estes critérios específicos. Serão fornecidas mais informações sobre estas noções nas Orientações sobre Definição de Perfis que o Grupo de Trabalho do Artigo 29.º apresentará futuramente.

¹² Ver considerando 71: «em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis».

¹³ Ver considerando 75: «quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas».

¹⁴ Ver, por exemplo, os considerandos 75, 76, 92 e 116.

3. Controlo sistemático: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um «*controlo sistemático de zonas acessíveis ao público*» (artigo 35.º, n.º 3, alínea c))¹⁵. Este tipo de controlo é um critério porque os dados pessoais podem ser recolhidos em circunstâncias em que os titulares dos dados podem não estar cientes de quem está a recolher os seus dados e da forma como esses dados serão utilizados. Adicionalmente, pode ser impossível para os indivíduos evitarem estar sujeitos a este tipo de tratamento em espaço(s) público(s) (ou zonas acessíveis ao público).
4. Dados sensíveis ou dados de natureza altamente pessoal: inclui categorias especiais de dados pessoais, tal como definido no artigo 9.º (por exemplo, informações acerca das opiniões políticas dos indivíduos), bem como dados pessoais relacionados com condenações penais e infrações, tal como definido no artigo 10.º. Um exemplo seria um hospital geral que mantenha registos médicos dos doentes ou um investigador privado que mantenha informações acerca dos autores das infrações. Para além destas disposições do RGPD, algumas categorias de dados podem ser consideradas como categorias que aumentam os possíveis riscos para os direitos e as liberdades dos indivíduos. Estes dados pessoais são considerados sensíveis (na aceção comum deste termo) porque estão associados a atividades privadas e familiares (tais como comunicações eletrónicas cuja confidencialidade deve ser protegida) ou porque afetam o exercício de um direito fundamental (tais como dados de localização cuja recolha põe em causa a liberdade de circulação) ou porque a sua violação implica claramente que a vida quotidiana do titular dos dados será gravemente afetada (tais como dados financeiros que possam ser utilizados numa fraude de pagamentos). A este respeito, pode ser relevante saber se os dados já foram tornados públicos pelo titular dos dados ou por terceiros. O facto de os dados pessoais já terem sido tornados públicos pode ser considerado um fator pertinente para avaliar se, possivelmente, os dados seriam ou não utilizados para determinados fins. Este critério pode também incluir dados como documentos pessoais, mensagens de correio eletrónico, diários, notas de dispositivos eletrónicos de leitura equipados com funções de introdução de notas, bem como informações muito pessoais incluídas em aplicações onde ficam registados eventos da vida dos indivíduos.
5. Dados tratados em grande escala: o RGPD não define o que constitui grande escala, contudo o considerando 91 fornece alguma orientação. Em qualquer caso, o Grupo de Trabalho do Artigo 29.º recomenda que os seguintes fatores, em especial, sejam considerados quando se determina se o tratamento é ou não efetuado em grande escala¹⁶:
 - a. o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;
 - b. o volume de dados e/ou a diversidade de dados diferentes a tratar;

¹⁵ O Grupo de Trabalho do Artigo 29.º interpreta «*sistemático*» como significando um ou mais dos seguintes pontos (ver as orientações do Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/EN WP 243):

- que ocorre de acordo com um sistema;
- pré-determinado, organizado ou metódico;
- que acontece como parte de um plano geral de recolha de dados;
- realizado como parte de uma estratégia.

O Grupo de Trabalho do Artigo 29.º interpreta «*zona acessível ao público*» como sendo qualquer local aberto a qualquer membro do público, por exemplo, uma praça, um centro comercial, uma rua, um mercado, uma estação de comboios ou uma biblioteca pública.

¹⁶ Ver as orientações do Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/EN WP 243.

- c. a duração da atividade de tratamento de dados ou a sua pertinência;
 - d. a dimensão geográfica da atividade de tratamento.
6. Estabelecer correspondências ou combinar conjuntos de dados: por exemplo, com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados¹⁷.
 7. Dados relativos a titulares de dados vulneráveis (considerando 75): o tratamento deste tipo de dados constitui um critério devido ao acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, significando isto que os indivíduos podem não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos. Os titulares de dados vulneráveis podem incluir crianças (estas podem ser consideradas incapazes de consentir ou opor-se consciente e criteriosamente ao tratamento dos seus dados), empregados, segmentos mais vulneráveis da população que necessitem de proteção especial (pessoas com doenças mentais, requerentes de asilo, idosos, doentes, etc.) e todos os casos em que possa ser identificado um desequilíbrio na relação entre a posição do titular dos dados e o responsável pelo tratamento.
 8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais, tais como combinar a utilização da impressão digital e do reconhecimento facial para melhorar o controlo do acesso físico, etc. O RGPD deixa claro (artigo 35.º, n.º 1, e considerando 89 e 91) que a utilização de uma nova tecnologia, definida em «conformidade com o nível de conhecimentos tecnológicos alcançado» (considerando 91), pode desencadear a necessidade de realização de uma AIPD. Isto acontece porque a utilização dessa tecnologia pode envolver novas formas de recolha e utilização de dados, possivelmente com elevado risco para os direitos e as liberdades dos indivíduos. Na verdade, as consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas. Uma AIPD ajudará o responsável pelo tratamento de dados a compreender e dar resposta a esses riscos. Por exemplo, algumas aplicações da «Internet das Coisas» podem ter um impacto significativo na vida quotidiana e na privacidade dos indivíduos e, como tal, exigem a realização de uma AIPD.
 9. Quando o próprio tratamento *impede os titulares dos dados «de exercer um direito ou de utilizar um serviço ou um contrato»* (artigo 22.º e considerando 91). Estão incluídas operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato. Um exemplo disto é quando um banco faz um controlo seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário com vista a decidir se lhes concede ou não um empréstimo.

Na maioria dos casos, o responsável pelo tratamento de dados pode considerar que um tratamento que satisfaça dois critérios exige a realização de uma AIPD. Em geral, o Grupo de Trabalho do Artigo 29.º considera que quantos mais critérios forem satisfeitos pelo tratamento maior é a probabilidade de este implicar um elevado risco para os direitos e as liberdades dos titulares dos dados e, por conseguinte, de necessitar de uma AIPD, independentemente das medidas que o responsável pelo tratamento pretender adotar.

¹⁷ Ver explicação no parecer do Grupo de Trabalho do Artigo 29.º sobre a limitação das finalidades 13/EN WP 203, p. 24.

Contudo, em alguns casos, **um responsável pelo tratamento de dados pode considerar que um tratamento que satisfaça apenas um dos critérios exige a realização de uma AIPD.**

Os exemplos apresentados a seguir ilustram a forma como os critérios devem ser utilizados para avaliar se uma operação de tratamento específica exige ou não uma AIPD:

Exemplos de tratamento	Crítérios pertinentes possíveis	Exige-se a realização de uma AIPD?
Um hospital que faz o tratamento dos dados genéticos e de saúde dos seus doentes (sistema de informação do hospital).	<ul style="list-style-type: none"> - <u>Dados sensíveis ou dados de natureza altamente pessoal.</u> - Dados relativos a titulares de dados vulneráveis. - Dados tratados em grande escala. 	Sim
Utilização de um sistema de câmaras para controlar o comportamento dos condutores nas autoestradas. O responsável pelo tratamento pretende utilizar um sistema inteligente de análise através de vídeo para seleccionar carros específicos e reconhecer automaticamente as matrículas.	<ul style="list-style-type: none"> - Controlo sistemático. - Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais. 	
Uma empresa que controle sistematicamente as atividades dos seus empregados, incluindo o controlo dos computadores, da atividade internet, etc. dos seus empregados.	<ul style="list-style-type: none"> - Controlo sistemático. - Dados relativos a titulares de dados vulneráveis. 	
Recolha de dados públicos das redes sociais para elaborar perfis.	<ul style="list-style-type: none"> - Avaliação ou classificação. - Dados tratados em grande escala. - Estabelecer correspondências ou combinar conjuntos de dados. - <u>Dados sensíveis ou dados de natureza altamente pessoal:</u> 	
Uma instituição que crie uma base de dados a nível nacional de notação de crédito ou de fraude.	<ul style="list-style-type: none"> - Avaliação ou classificação. - Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar. - Impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato. - <u>Dados sensíveis ou dados de natureza altamente pessoal:</u> 	
Conservação para fins de arquivo de dados pessoais sensíveis pseudonimizados relativos a titulares de dados vulneráveis que tenham participado em projetos de investigação ou ensaios clínicos.	<ul style="list-style-type: none"> - Dados sensíveis. - Dados relativos a titulares de dados vulneráveis. - Impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato. 	

Exemplos de tratamento	Crítérios pertinentes possíveis	Exige-se a realização de uma AIPD?
Tratamento de «dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado» (considerando 91).	<ul style="list-style-type: none"> - <u>Dados sensíveis ou dados de natureza altamente pessoal.</u> - Dados relativos a titulares de dados vulneráveis. 	Não
Revista em linha que utilize uma lista de endereços de correio eletrónico para enviar fascículos diários genéricos da revista para os seus subscritores.	<ul style="list-style-type: none"> - Dados tratados em grande escala. 	
Um sítio web de comércio em linha que mostre anúncios de peças de automóveis antigos envolvendo a utilização limitada de perfis com base nos itens visualizados ou comprados no seu próprio sítio web.	<ul style="list-style-type: none"> - Avaliação ou classificação. 	

Em contrapartida, uma operação de tratamento pode corresponder aos casos supramencionados e continuar a ser considerada pelo responsável pelo tratamento como uma operação que não é «suscetível de implicar um elevado risco». Nestes casos, o responsável pelo tratamento deve justificar e documentar as razões que o levam a não realizar uma AIPD e incluir/registar os pontos de vista do encarregado da proteção de dados.

Adicionalmente, como parte do princípio da responsabilização, cada responsável pelo tratamento de dados «*conserva um registo de todas as atividades de tratamento sob a sua responsabilidade*», onde constam, entre outros, as finalidades do tratamento dos dados, a descrição das categorias de titulares de dados e das categorias de dados pessoais e «*[s]e possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1*» (artigo 30.º, n.º 1) e deve avaliar a probabilidade de ser suscetível de implicar um elevado risco, mesmo que acabem por decidir não realizar uma AIPD.

Nota: exige-se que as autoridades de controlo elaborem, tornem pública e comuniquem uma lista das operações de tratamento sujeitas ao requisito de AIPD ao Comité Europeu para a Proteção de Dados (CEPD) (artigo 35.º, n.º 4)¹⁸. Os critérios definidos acima podem ajudar as autoridades de controlo a elaborar esta lista, podendo ser posteriormente acrescentado conteúdo mais específico se tal for adequado. Por exemplo, o tratamento de qualquer tipo de dados biométricos ou de dados referentes a crianças também pode ser considerado como pertinente para o desenvolvimento de uma lista nos termos do artigo 35.º, n.º 4.

- b) Quando é que uma AIPD não é obrigatória? Quando o tratamento não for «*suscetível de implicar um elevado risco*», quando já existir uma AIPD semelhante, quando tiver sido autorizado antes de maio de 2018, quando tiver um fundamento jurídico ou

¹⁸ Nesse contexto, «*a autoridade de controlo competente aplica o procedimento de controlo da coerência referido no artigo 63.º sempre que essas listas enunciem atividades de tratamento relacionadas com a oferta de bens ou serviços a titulares de dados ou com o controlo do seu comportamento em diversos Estados-Membros, ou possam afetar substancialmente a livre circulação de dados pessoais na União*» (artigo 35.º, n.º 6).

quando fizer parte de uma lista de operações de tratamento para as quais não seja necessária uma AIPD.

O Grupo de Trabalho do Artigo 29.º considera que uma AIPD não é obrigatória nos seguintes casos:

- **quando o tratamento não for «suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares»** (artigo 35.º, n.º 1);
- **quando a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada uma AIPD.** Nestes casos, podem ser utilizados os resultados da AIPD realizada para o tratamento semelhante (artigo 35.º, n.º 1¹⁹);
- quando as operações de tratamento tiverem sido previamente controladas por uma autoridade de controlo antes de maio de 2018 em condições específicas que não se tenham alterado²⁰ (ver III.C);
- **quando uma operação de tratamento, nos termos do artigo 6.º, n.º 1, alíneas c) ou e), tiver um fundamento jurídico no direito da UE ou de um Estado-Membro, em que o direito regule a operação de tratamento específica e em que a AIPD já tenha sido realizada** como parte da adoção desse fundamento jurídico (artigo 35.º, n.º 10)²¹, salvo se o Estado-Membro considerar necessário proceder a essa avaliação antes das atividades de tratamento;
- **quando o tratamento estiver incluído na lista opcional (definida pela autoridade de controlo) de operações de tratamento** para as quais não é obrigatória uma AIPD (artigo 35.º, n.º 5). A referida lista pode conter atividades de tratamento que satisfazem as condições especificadas por esta autoridade, em especial através de orientações, decisões ou autorizações específicas, regras de conformidade, etc. (p. ex. em França, autorizações, isenções, regras simplificadas, pacotes de conformidade, ...). Nestes casos, e sujeito a uma reavaliação pela autoridade de controlo competente, não é obrigatório realizar uma AIPD, mas somente se o tratamento se enquadrar estritamente no âmbito do procedimento pertinente mencionado na lista e continuar a estar totalmente em conformidade com todos os requisitos pertinentes do RGPD.

C. E relativamente às operações de tratamento já existentes? As AIPD são obrigatórias nalgumas circunstâncias.

A obrigação de realizar uma AIPD é aplicável às operações de tratamento existentes suscetíveis de implicar um elevado risco para os direitos e as liberdades das pessoas singulares e em relação às quais não tenha havido alteração dos riscos, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

¹⁹ «Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação».

²⁰ «As decisões da Comissão que tenham sido adotadas e as autorizações que tenham sido emitidas pelas autoridades de controlo com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas» (considerando 171).

²¹ Quando é realizada aquando da adoção da legislação que serve de fundamento jurídico ao tratamento, a AIPD é suscetível de requerer um controlo antes de se começarem as operações, uma vez que a legislação adotada pode diferir da proposta de maneira que afete a privacidade e a proteção dos dados. Além disso, podem não estar disponíveis suficientes pormenores técnicos em relação ao tratamento propriamente dito à data da adoção da legislação, mesmo que tenha sido acompanhada por uma AIPD. Nestes casos, pode ainda ser necessário realizar uma AIPD específica antes de se realizarem as atividades de tratamento propriamente ditas.

Não é necessário realizar uma AIPD para operações de tratamento que tenham sido previamente controladas por uma autoridade de controlo ou pelo encarregado da proteção de dados, em conformidade com o artigo 20.º da Diretiva 95/46/CE, e que sejam realizadas sem alterações desde o controlo prévio anterior. Na verdade, *«[a]s decisões da Comissão que tenham sido adotadas e as autorizações que tenham emitidas pelas autoridades de controlo com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas»* (considerando 171).

Em contrapartida, isto significa que qualquer tratamento de dados cujas condições de aplicação (âmbito, finalidade, recolha de dados pessoais, identidade dos responsáveis pelo tratamento dos dados ou dos destinatários, período de retenção dos dados, medidas técnicas e organizativas, etc.) tenham mudado desde o controlo prévio realizado pela autoridade de controlo ou pelo encarregado da proteção dos dados e que sejam suscetíveis de implicar um elevado risco devem ser sujeitas a uma AIPD.

Além disso, pode ser obrigatório realizar uma AIPD após uma alteração dos riscos decorrentes das operações de tratamento²², por exemplo, porque se começou a utilizar uma nova tecnologia ou porque os dados pessoais passaram a ser utilizados para uma finalidade diferente. As operações de tratamento de dados podem evoluir rapidamente e podem surgir novas vulnerabilidades. Por conseguinte, importa referir que a revisão de uma AIPD não é apenas útil para fins de melhoria contínua, trata-se de algo fundamental para manter o nível de proteção dos dados num ambiente em permanente mudança. Uma AIPD também pode tornar-se necessária pelo facto de o contexto organizacional ou societal da atividade de tratamento ter mudado, por exemplo, porque os efeitos de determinadas decisões automatizadas se tornaram mais significativos ou porque novas categorias de titulares de dados ficaram vulneráveis a discriminação. Cada um destes exemplos pode ser um elemento que conduz a uma alteração do risco decorrente da atividade de tratamento em causa.

Em contrapartida, algumas alterações também podem fazer baixar os riscos. Por exemplo, uma operação de tratamento pode evoluir no sentido de as decisões deixarem de ser automatizadas ou então uma atividade de controlo deixa de ser sistemática. Neste caso, a revisão da análise do risco efetuada pode revelar que a realização de uma AIPD deixa de ser obrigatória.

Por uma questão de boa prática, **uma AIPD deve ser continuamente revista e regularmente reavaliada**. Por conseguinte, mesmo que não seja obrigatória a realização de uma AIPD em 25 de maio de 2018, será necessário, na altura adequada, que o responsável pelo tratamento realize essa AIPD como parte das suas obrigações gerais em matéria de responsabilização.

D. Como realizar uma AIPD?

a) Em que altura deve ser realizada uma AIPD? Antes de se iniciar o tratamento.

A AIPD deve ser realizada «antes de iniciar o tratamento» (artigo 35.º, n.ºs 1 e 10, e considerando 90 e 93)²³. Verifica-se a coerência com os princípios da proteção de dados desde a

²² Em termos de contexto, recolha de dados, finalidades, funcionalidade, dados pessoais tratados, destinatários, combinações de dados, riscos (ativos subjacentes, fontes de riscos, impactos potenciais, ameaças, etc.), medidas de segurança e transferências internacionais.

²³ Exceto quando se trata de um tratamento já existente e que foi previamente controlado pela autoridade de controlo, caso em que a AIPD deve ser realizada antes de se efetuarem alterações significativas.

conceção e por defeito (artigo 25.º e considerando 78). A AIPD deve ser encarada como um instrumento de apoio à tomada de decisão em relação ao tratamento.

A AIPD deve ser iniciada o mais cedo possível na conceção da operação de tratamento, mesmo que algumas das operações de tratamento ainda sejam desconhecidas. A atualização da AIPD ao longo do ciclo de vida do projeto garantirá que a proteção dos dados e a privacidade serão consideradas e incentivará a criação de soluções que promovem a conformidade. Pode também ser necessário repetir as etapas individuais da avaliação à medida que o processo de desenvolvimento progride, uma vez que a seleção de determinadas medidas técnicas ou organizacionais pode afetar a gravidade dos riscos colocados pelo tratamento ou a probabilidade de estes se concretizarem.

O facto de a AIPD poder necessitar de ser atualizada após o tratamento ter efetivamente sido iniciado não é uma razão válida para adiar ou não realizar uma AIPD. A AIPD é um processo contínuo, especialmente quando uma operação de tratamento é dinâmica e está sujeita a mudanças permanentes. **A realização de uma AIPD é um processo contínuo e não um exercício que acontece uma única vez.**

- b) Quem está obrigado a realizar uma AIPD? O responsável pelo tratamento, com o encarregado do tratamento dos dados e os subcontratantes.

O responsável pelo tratamento é responsável por garantir a realização da AIPD (artigo 35.º, n.º 2). A realização da AIPD pode ser efetuada por outrem, dentro ou fora da organização, mas o responsável pelo tratamento continua a ser o responsável último por essa tarefa.

O responsável pelo tratamento deve também solicitar o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado (artigo 35.º, n.º 2), sendo que o seu parecer e as decisões tomadas pelo responsável pelo tratamento devem ser documentadas na AIPD. O encarregado da proteção de dados pode igualmente controlar a realização da AIPD (artigo 39.º, n.º 1, alínea c)). Para mais esclarecimentos, consultar as orientações do Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/EN WP 243.

Se o tratamento for total ou parcialmente efetuado por um subcontratante, **o subcontratante deve auxiliar o responsável pelo tratamento na realização da AIPD** e fornecer todas as informações necessárias (em consonância com o artigo 28.º, n.º 3, alínea f)).

O responsável pelo tratamento «solicita a opinião dos titulares de dados ou dos seus representantes» (artigo 35.º, n.º 9), «[s]e for adequado». O Grupo de Trabalho do Artigo 29.º considera que:

- essas opiniões podem ser solicitadas através de uma variedade de meios, dependendo do contexto (p. ex. um estudo genérico relacionado com a finalidade e os meios da operação de tratamento, uma questão colocada aos representantes do pessoal ou os habituais inquéritos enviados aos futuros clientes do responsável pelo tratamento dos dados), assegurando que o responsável pelo tratamento tem legitimidade para tratar quaisquer dados pessoais envolvidos na obtenção dessas opiniões. Importa referir, contudo, que o consentimento para o tratamento não é obviamente uma forma de solicitar as opiniões dos titulares dos dados;
- se a decisão final do responsável pelo tratamento de dados for diferente das opiniões dos titulares dos dados, as razões que o levam a prosseguir ou não devem ser documentadas;
- o responsável pelo tratamento também deve documentar a sua justificação para não solicitar opiniões aos titulares dos dados, caso decida que tal não é adequado, por exemplo, se ao fazê-

lo comprometer a confidencialidade dos planos de negócio das empresas ou se tal procedimento for desproporcionado ou impraticável.

Por último, considera-se ser boa prática definir e documentar outros papéis e responsabilidades específicos, dependendo da política, dos processos e das regras praticados internamente, por exemplo,

- quando unidades comerciais específicas se propuserem a realizar uma AIPD, essas unidades devem então fornecer dados para a AIPD e devem participar no processo de validação da AIPD;
- se for adequado, é recomendável solicitar pareceres a peritos independentes de profissões diferentes²⁴ (advogados, peritos em TI, peritos em segurança, sociólogos, peritos em deontologia, etc.).
- os papéis e as responsabilidades dos subcontratantes devem ser definidos contratualmente; e a AIPD deve ser realizada com a ajuda do subcontratante, tendo em conta a natureza do tratamento e as informações ao dispor do subcontratante (artigo 28.º, n.º 3, alínea f));
- o Diretor da Segurança das Informações, caso seja designado, bem como o encarregado da proteção dos dados, pode sugerir ao responsável pelo tratamento a realização de uma AIPD a uma operação de tratamento específica, e deve ajudar as partes interessadas em relação à metodologia, ajudar a aferir a qualidade da avaliação do risco e se o risco residual é aceitável, bem como desenvolver conhecimentos específicos em relação ao contexto do responsável pelo tratamento de dados;
- o Diretor da Segurança das Informações, caso seja designado, e/ou o departamento de TI, deve prestar assistência ao responsável pelo tratamento e pode propor a realização de uma AIPD a uma operação de tratamento específica, dependendo das necessidades de segurança ou operacionais.

- c) Qual é a metodologia para realizar uma AIPD? Existem metodologias diferentes, mas os critérios são comuns.

²⁴ *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3: [Recomendações para um quadro de avaliação de impacto na privacidade na União Europeia, Prestação D3]*
http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

O RGPD define os elementos mínimos de uma AIPD (artigo 35.º, n.º 7, e considerando 84 e 90):

- «[u]ma descrição das operações de tratamento previstas e a finalidade do tratamento»;
- «[u]ma avaliação da necessidade e proporcionalidade das operações de tratamento»;
- «[u]ma avaliação dos riscos para os direitos e liberdades dos titulares dos dados»;
- «[a]s medidas previstas para»
 - «fazer face aos riscos»;
 - «demonstrar a conformidade com o presente regulamento».

A figura seguinte ilustra o processo iterativo genérico para a realização de uma AIPD²⁵:



Ao avaliar o impacto de uma operação de tratamento de dados, deve ser tido na devida conta (artigo 35.º, n.º 8) o cumprimento de um código de conduta (artigo 40.º). Isto pode ser útil para demonstrar que foram escolhidas ou aplicadas medidas adequadas, desde que o código de conduta seja adequado para a operação de tratamento. Importa ter em conta as certificações, os selos e as marcas para efeitos de demonstração da conformidade com o RGPD das operações de tratamento de responsáveis pelo tratamento e subcontratantes (artigo 42.º), bem como regras vinculativas aplicáveis às empresas.

Todos os requisitos pertinentes definidos no RGPD preveem um quadro alargado e genérico para a elaboração e realização de uma AIPD. A execução prática de uma AIPD depende dos requisitos definidos no RGPD que podem ser complementados com orientações práticas mais pormenorizadas. Por conseguinte, a execução da AIPD é dimensionável. Significa isto que mesmo um pequeno responsável pelo tratamento de dados pode conceber e executar uma AIPD adequada para as suas operações de tratamento.

²⁵ Importa sublinhar que o processo descrito nesta figura é iterativo: na prática, é provável que cada uma das etapas seja revisitada várias vezes antes de a AIPD poder ser concluída.

O considerando 90 do RGPD enuncia vários elementos da AIPD que se sobrepõem a elementos bem definidos da gestão do risco (p. ex. ISO 31000²⁶). Em matéria de gestão dos riscos, uma AIPD destina-se a «gerir os riscos» para os direitos e as liberdades das pessoas singulares, utilizando os seguintes processos:

- estabelecendo o contexto: «*tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco*»;
- avaliando os riscos: «*avaliar a probabilidade ou gravidade particulares do elevado risco*»;
- dando resposta aos riscos: «*atenuar esse risco*» e «*assegurar a proteção dos dados pessoais*» e «*comprovar a observância do presente regulamento*».

Nota: a AIPD ao abrigo do RGPD é um instrumento que visa gerir os riscos para os direitos dos titulares dos dados e, como tal, avalia-os na perspetiva destes últimos, como acontece em determinados domínios (p. ex. segurança societal). Em contrapartida, a gestão dos riscos noutros domínios (p. ex. segurança da informação) centra-se na organização.

O RGPD dá aos responsáveis pelo tratamento de dados a flexibilidade necessária para determinar a estrutura e a forma precisas da AIPD com vista a que esta se encaixe nas práticas de trabalho existentes. Existem vários processos diferentes na UE e a nível mundial que têm em conta os elementos descritos no considerando 90. Contudo, seja qual for a sua forma, uma AIPD deve avaliar genuinamente os riscos, permitindo assim que os responsáveis pelo tratamento tomem medidas para dar resposta a esses riscos.

Podem ser utilizadas diferentes metodologias (no anexo 1, ver exemplos de metodologias de proteção de dados e de avaliação de impacto na privacidade) para ajudar a implementar os requisitos básicos definidos no RGPD. Com vista a permitir a existência destas abordagens diferentes, permitindo ao mesmo tempo que os responsáveis pelo tratamento cumpram o RGPD, foram identificados critérios comuns (ver anexo 2). Estes critérios clarificam os requisitos básicos do regulamento, mas o seu âmbito é suficientemente amplo para permitir diferentes formas de implementação. Podem ser utilizados para demonstrar que uma determinada metodologia de AIPD cumpre as normas exigidas pelo RGPD. **Cabe ao responsável pelo tratamento de dados escolher uma metodologia, mas esta metodologia deve estar em conformidade com os critérios previstos no anexo 2.**

No que toca às AIPD, o Grupo de Trabalho do Artigo 29.º incentiva o desenvolvimento de quadros específicos para cada setor. Isto porque podem tirar partido de conhecimentos setoriais específicos, o que quer dizer que a AIPD pode responder às especificidades de determinado tipo de operação de tratamento (p. ex. determinados tipos de dados, ativos empresariais, impactos potenciais, ameaças, medidas). Significa isto que a AIPD pode abordar os problemas que surgem num determinado setor económico ou quando se utilizam determinadas tecnologias ou quando se realizam determinados tipos de operações de tratamento.

Por último, se necessário, «*o responsável pelo tratamento procede a um controlo para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados, pelo*

²⁶ Processos de gestão dos riscos: comunicação e consulta, estabelecer o contexto, avaliação dos riscos, resposta aos riscos, monitorização e reexame (ver termos e condições, bem como índice, da ISO 31000 em: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en>).

menos quando haja uma alteração dos riscos que as operações de tratamento representam» (artigo 35.º, n.º 11²⁷).

- d) Existe uma obrigação de publicar a AIPD? Não, mas a publicação de um resumo pode fomentar a confiança, e a AIPD completa deve ser comunicada à autoridade de controlo em caso de consulta prévia ou se tal for solicitado pela autoridade de proteção de dados.

A publicação de uma AIPD não é um requisito jurídico do RGPD, essa decisão recai sobre o responsável pelo tratamento. Contudo, os responsáveis pelo tratamento devem considerar, pelo menos, a publicação parcial da AIPD, por exemplo, um resumo ou uma conclusão.

A finalidade dessa publicação parcial seria ajudar a fomentar a confiança nas operações de tratamento do responsável pelo tratamento e demonstrar responsabilidade e transparência. Considera-se uma boa prática publicar uma AIPD quando os membros do público são afetados pela operação de tratamento. Acontece em especial quando a AIPD é realizada por uma autoridade pública.

Não é necessário que a AIPD publicada contenha a totalidade da avaliação, especialmente quando a AIPD pode conter informações específicas sobre riscos de segurança para o responsável pelo tratamento de dados ou revelar segredos comerciais ou informações comercialmente sensíveis. Nestas circunstâncias, a versão publicada pode consistir apenas num resumo das principais conclusões da AIPD ou até mesmo numa mera declaração de que foi realizada uma AIPD.

Além disso, quando uma AIPD apresenta elevados riscos residuais, exige-se que o responsável pelo tratamento de dados consulte previamente a autoridade de controlo antes de proceder ao tratamento (artigo 36.º, n.º 1). Como parte deste procedimento, a AIPD deve ser comunicada integralmente (artigo 36.º, n.º 3, alínea e)). A autoridade de controlo pode dar as suas orientações²⁸, não comprometendo segredos comerciais nem revelando vulnerabilidades de segurança, sujeito aos princípios aplicáveis em cada Estado-Membro em matéria de acesso público a documentos oficiais.

E. Quando deve a autoridade de controlo ser consultada? Quando os riscos residuais são elevados.

Como foi explicado anteriormente:

- a realização de uma AIPD é obrigatória quando uma operação de tratamento *«for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares»* (artigo 35.º, n.º 1, ver III.B.a). Por exemplo, o tratamento de dados de saúde em grande escala é considerado um tratamento suscetível de implicar um elevado risco, exigindo assim a realização de uma AIPD;
- depois, é da responsabilidade do responsável pelo tratamento de dados avaliar os riscos para os direitos e as liberdades dos titulares dos dados e identificar as medidas²⁹ previstas para reduzir esses riscos para um nível aceitável e demonstrar a conformidade com o RGPD

²⁷ O artigo 35.º, n.º 10, apenas exclui explicitamente a aplicação do artigo 35.º, n.ºs 1 a 7.

²⁸ As orientações por escrito destinadas ao responsável pelo tratamento só são necessárias quando a autoridade de controlo considerar que o tratamento previsto viola o regulamento nos termos do artigo 36.º, n.º 2.

²⁹ Incluindo ter em conta orientações existentes do Comité Europeu para a Proteção de Dados (CEPD) e das autoridades de controlo, bem como ter em conta o estado da arte e os custos de aplicação, tal como previsto no artigo 35.º, n.º 1.

(artigo 35.º, n.º 7, ver III.C.c). Um exemplo para a conservação de dados pessoais em computadores portáteis pode ser a utilização de medidas de segurança técnicas e organizacionais adequadas (cifragem total e eficaz do disco, gestão robusta de chaves, controlo de acesso adequado, ficheiros de segurança seguros, etc.), para além das políticas existentes (notificação, consentimento, direito de acesso, direito de objeção, etc.).

No exemplo dos computadores portáteis referido acima, se se considerar que os riscos foram suficientemente reduzidos pelo responsável pelo tratamento de dados e na aceção do artigo 36.º, n.º 1, e dos considerandos 84 e 94, é possível proceder ao tratamento sem consultar a autoridade de controlo. O responsável pelo tratamento dos dados deve consultar a autoridade de controlo nos casos em que não seja possível dar uma resposta cabal aos riscos identificados pelo responsável pelo tratamento de dados (ou seja, quando os riscos residuais permanecem elevados).

Exemplos de um risco residual inaceitavelmente elevado são os casos em que os titulares dos dados podem sofrer consequências significativas, ou mesmo irreversíveis, que podem não conseguir superar (p. ex. um acesso ilícito a dados que possam vir a constituir uma ameaça para a vida dos titulares dos dados, um despedimento, uma ameaça financeira) e/ou casos em que pareça óbvio que o risco se irá concretizar (p. ex. não ser possível reduzir o número de pessoas que podem aceder aos dados devido aos modos de partilha, utilização ou distribuição utilizados ou quando uma vulnerabilidade conhecida não é solucionada).

Sempre que o responsável pelo tratamento de dados não conseguir encontrar medidas suficientes para reduzir os riscos para um nível aceitável (ou seja, quando os riscos residuais permanecem elevados), é obrigatório consultar a autoridades de controlo³⁰.

Além disso, o responsável pelo tratamento deve consultar a autoridade de controlo sempre que o direito do Estado-Membro exija que os responsáveis pelo tratamento consultem a autoridade de controlo e/ou dela obtenham uma autorização prévia em relação ao tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública (artigo 36.º, n.º 5).

Contudo, importa referir que, independentemente de a consulta à autoridade de controlo ser ou não obrigatória com base no nível de risco residual, as obrigações que impõem a manutenção de um registo da AIPD e a atualização da AIPD em devido tempo permanecem válidas.

IV. Conclusões e recomendações

As AIPD são uma forma útil de os responsáveis pelo tratamento de dados aplicarem sistemas de tratamento de dados que estejam em conformidade com o RGPD, podendo ser obrigatórias para alguns tipos de operações de tratamento. São dimensionáveis e podem assumir diferentes formas, mas o RGPD define os requisitos básicos para uma AIPD eficaz. Os responsáveis pelo tratamento de dados devem encarar a realização de uma AIPD como uma atividade útil e positiva que ajuda à conformidade jurídica.

³⁰ Nota: «a pseudonimização e a cifragem dos dados pessoais» (bem como a minimização de dados, mecanismos de controlo, etc.) não são necessariamente medidas adequadas. São meros exemplos. As medidas adequadas dependem do contexto e dos riscos específicos das operações de tratamento.

O artigo 24.º, n.º 1, define a responsabilidade básica do responsável pelo tratamento em termos de conformidade com o RGPD: «[t]endo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.»

A AIPD contribui significativamente para a conformidade com o regulamento quando está planeado ou ocorre um tratamento de dados de elevado risco. Significa isto que os responsáveis pelo tratamento de dados devem utilizar os critérios definidos no presente documento para determinar se uma AIPD deve ou não ser realizada. A política interna seguida pelo responsável pelo tratamento de dados pode alargar esta lista para além dos requisitos jurídicos do RGPD. Resulta daqui uma maior confiança por parte dos titulares dos dados e dos outros responsáveis pelo tratamento de dados.

Quando estiver planeado um tratamento suscetível de implicar um elevado risco, o responsável pelo tratamento dos dados deve:

- escolher uma metodologia para a AIPD (exemplos no anexo 1) que satisfaça os critérios que constam do anexo 2 ou especificar e aplicar um processo sistemático de AIPD que:
 - o esteja em conformidade com os critérios que constam do anexo 2;
 - o esteja integrado em processos já existentes de conceção, desenvolvimento, alteração, reavaliação de risco e reavaliação operacional, em conformidade com os processos, o contexto e a cultura internos;
 - o envolva as partes interessadas adequadas e defina claramente as responsabilidades das mesmas (responsável pelo tratamento, encarregado da proteção de dados, titulares dos dados ou seus representantes, empresas, serviços técnicos, subcontratantes, diretor de segurança da informação, etc.);
- fornecer o relatório da AIPD à autoridade de controlo competente quando tal for solicitado;
- consultar a autoridade de controlo quando não tiver determinado medidas suficientes para atenuar os riscos elevados;
- reavaliar periodicamente a AIPD e o tratamento que esta avalia, pelo menos, quando houver uma alteração do risco colocado pelo tratamento da operação;
- documentar as decisões tomadas.

Anexo 1 — Exemplos de quadros existentes na UE em matéria de AIPD

O RGPD não especifica qual o processo de AIPD que deve ser utilizado, em vez disso permite que os responsáveis pelo tratamento de dados introduzam um quadro que complemente as suas práticas de trabalho já existentes, desde que tenham em conta os elementos enunciados no artigo 35.º, n.º 7. Esse quadro pode ser especificamente adaptado ao responsável pelo tratamento de dados ou comum a determinada indústria. Nos quadros de proteção de dados previamente publicados e desenvolvidos pelas autoridades de proteção de dados da UE e nos quadros de proteção de dados específicos por setor incluem-se (entre outros):

Exemplos de quadros de proteção de dados genéricos da UE:

- DE: Standard Data Protection Model [Modelo normalizado de proteção de dados], V.1.0 – versão experimental, 2016³¹.
https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
<https://www.cnil.fr/fr/node/15798>
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

Exemplos de quadros de proteção de dados da UE específicos por setor:

- Quadro para as avaliações do impacto das aplicações RFID na proteção da privacidade e dos dados³².
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Modelo de avaliação do impacto na proteção de dados no contexto das redes inteligentes e dos sistemas de contadores inteligentes³³

³¹ Reconhecido unanimemente e favoravelmente (com abstenção da Bavaria) pela 92.ª Conferência das Autoridades de Proteção de Dados Independentes de Bund e Länder em Kühlungsborn nos dias 9 e 10 de novembro de 2016.

³² Ver igualmente:

- Recomendação da Comissão, de 12 de maio de 2009, relativa à aplicação dos princípios de proteção da privacidade e dos dados nas aplicações assentes na identificação por radiofrequências.
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2009%3A122%3A0047%3A0051%3APT%3APDF>
- Parecer 9/2011 sobre a proposta revista da indústria relativa a um quadro para as avaliações do impacto das aplicações RFID na proteção da privacidade e dos dados.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_pt.pdf

³³ Ver também o Parecer 07/2013 sobre o modelo de avaliação de impacto em matéria de proteção de dados para as redes inteligentes e os sistemas de contadores inteligentes («modelo de AIPD») elaborado pelo Grupo de

http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Uma norma internacional também pode fornecer orientações relativas às metodologias utilizadas para realizar uma AIPD (ISO/IEC 29134³⁴).

Peritos 2 da Task Force da Comissão para as redes inteligentes. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_pt.pdf

³⁴ ISO/IEC 29134 (projeto), *Information technology – Security techniques – Privacy impact assessment – Guidelines* [Tecnologia da Informação – Técnicas de segurança – Avaliação de impacto na privacidade – Orientações], Organização Internacional de Normalização (ISO).

Anexo 2 — Critérios para uma AIPD aceitável

O Grupo de Trabalho do Artigo 29.º propõe os seguintes critérios que os responsáveis pelo tratamento dos dados podem utilizar para avaliar se uma AIPD, ou uma metodologia para realizar uma AIPD, é ou não suficientemente exaustiva para estar em conformidade com o RGPD:

- ☐ uma descrição sistemática das operações de tratamento é fornecida (artigo 35.º, n.º 7, alínea a)):
 - ☐ a natureza, o âmbito, o contexto e as finalidades do tratamento são tidos em conta (considerando 90);
 - ☐ os dados pessoais, os destinatários e o período de tempo durante o qual os dados pessoais serão conservados são registados;
 - ☐ uma descrição funcional da operação de tratamento é fornecida;
 - ☐ os ativos de que dependem os dados pessoais (equipamento informático, programa informático, redes, pessoas, papel ou canais de transmissão em papel) são identificados;
 - ☐ o cumprimento dos códigos de conduta aprovados é tida em conta (artigo 35.º, n.º 8);
- ☐ a necessidade e a proporcionalidade são avaliadas (artigo 35.º, n.º 7, alínea b)):
 - ☐ as medidas previstas para demonstrar a conformidade com o regulamento são determinadas (artigo 35.º, n.º 7, alínea d), e considerando 90), tendo em conta:
 - ☐ as medidas que contribuem para a proporcionalidade e a necessidade do tratamento com base em:
 - ☐ finalidade(s) determinada(s), explícita(s) e legítima(s) (artigo 5.º, n.º 1, alínea b));
 - ☐ licitude do tratamento (artigo 6.º);
 - ☐ dados adequados, pertinentes e limitados ao que é necessário (artigo 5.º, n.º 1, alínea c));
 - ☐ conservação por tempo limitado (artigo 5.º, n.º 1, alínea e));
 - ☐ as medidas que contribuem para os direitos dos titulares dos dados:
 - ☐ informações fornecidas ao titular dos dados (artigos 12.º, 13.º e 14.º);
 - ☐ direito de acesso e de portabilidade dos dados (artigos 15.º e 20.º);
 - ☐ direito de retificação e de apagamento dos dados (artigos 16.º, 17.º e 19.º);
 - ☐ direito de oposição e direito à limitação do tratamento (artigos 18.º, 19.º e 21.º);
 - ☐ relações com os subcontratantes (artigo 28.º);
 - ☐ garantias relativas às transferências internacionais (capítulo V);
 - ☐ consulta prévia (artigo 36.º).
- ☐ os riscos para os direitos e as liberdades dos titulares dos dados são geridos (artigo 35.º, n.º 7, alínea c)):
 - ☐ a origem, a natureza, a particularidade e a gravidade dos riscos são apreciadas (cf. considerando 84) ou, mais especificamente, para cada risco (acesso ilegítimo, modificação indesejada, desaparecimento de dados) da perspetiva dos titulares dos dados:
 - ☐ as fontes de risco são tidas em conta (considerando 90);
 - ☐ os potenciais impactos nos direitos e nas liberdades dos titulares dos dados são identificados na eventualidade de acesso ilegítimo, modificação indesejada e desaparecimento de dados, entre outros;
 - ☐ as ameaças que possam conduzir a acesso ilegítimo, modificação indesejada e desaparecimento de dados são identificadas;
 - ☐ a probabilidade e a gravidade são estimadas (considerando 90);
 - ☐ as medidas previstas para fazer face a esses riscos são determinadas (artigo 35.º, n.º 7, alínea d), e considerando 90);
- ☐ as partes interessadas são envolvidas:

- ☐ o parecer do encarregado da proteção de dados é solicitado (artigo 35.º, n.º 2);
- ☐ as opiniões dos titulares de dados ou dos seus representantes são solicitadas, se necessário (artigo 35.º, n.º 9).