

14 de novembro de 2017

Magda Cocco | [mpc@vda.pt](mailto:mpc@vda.pt)  
Inês Antas de Barros | [iab@vda.pt](mailto:iab@vda.pt)  
Carolina Moniz Pina | [cmz@vda.pt](mailto:cmz@vda.pt)

## PRIVACIDADE, PROTEÇÃO DE DADOS E CIBERSEGURANÇA

### GUIDELINES DO GRUPO DE TRABALHO DO ARTIGO 29 SOBRE O RGPD

A pouco mais de 6 meses para a aplicação do Regulamento Geral sobre a Proteção de Dados (“RGPD”) – em 25 de maio de 2018 –, o Grupo de Trabalho do Artigo 29 (“GT29”) adotou recentemente um conjunto de orientações sobre a aplicação de coimas, decisões automatizadas e definição de perfis e ainda sobre violações de dados pessoais.

Estas orientações visam concretizar e detalhar algumas disposições do RGPD, tal como já tinha sucedido com as orientações já emitidas sobre o Data Protection Officer, o Direito à Portabilidade, a Autoridade de Controlo Principal e os Data Protection Impact Assessments.

#### 1. ORIENTAÇÕES REFERENTES À APLICAÇÃO DE COIMAS

Nestas Orientações ([Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, wp253](#)), que se encontram em consulta pública até 28 de novembro de 2017, o GT29 vem esclarecer que as autoridades nacionais de controlo deverão proceder à avaliação dos factos que originaram o incumprimento, bem como das consequências decorrentes do mesmo, por forma a determinar quais as ferramentas mais adequadas para dar resposta à situação.

O GT29 avança ainda com algumas recomendações que deverão ser consideradas pelas autoridades de controlo aquando da decisão de aplicação de uma coima e o respetivo montante, à luz dos critérios previstos no RGPD, destacando-se as seguintes:

- Deverá ser atendida a natureza da violação de dados em causa, o âmbito e finalidade do tratamento, a adoção em tempo útil de medidas adequadas a bloquear a violação ou extensão dos efeitos da violação, bem como o número de titulares dos dados afetados pela violação e o impacto da mesma.
- A duração da violação de dados poderá ser ilustrativa de elementos a ponderar, nomeadamente, (i) da existência ou não de dolo por parte do responsável pelo tratamento; (ii) da não adoção das medidas preventivas adequadas; ou (iii) da não aplicação das medidas técnicas e organizativas necessárias para o efeito e legalmente impostas (“comportamento responsável”).

[www.vda.pt](http://www.vda.pt)

Esta informação é de distribuição reservada e não deve ser entendida como qualquer forma de publicidade, pelo que se encontra vedada a sua cópia ou circulação. A informação proporcionada e as opiniões expressas são de carácter geral, não substituindo o recurso a aconselhamento jurídico adequado para a resolução de casos concretos.

VdA Legal Partners é uma rede internacional de prestação de serviços jurídicos que integra advogados autorizados a exercer advocacia nas jurisdições envolvidas, em conformidade com as regras legais e deontológicas aplicáveis em cada uma das jurisdições.

This is a limited distribution and should not be considered to constitute any kind of advertising. The reproduction or circulation thereof is prohibited. All information contained herein and all opinions expressed are of a general nature and are not intended to substitute recourse to expert legal advice for the resolution of real cases.

VdA Legal Partners is an international legal network comprising attorneys admitted in all the jurisdictions covered in accordance with the legal and statutory provisions applicable in each jurisdiction.

- Quanto ao grau de responsabilidade do responsável, em função das medidas técnicas ou organizativas implementadas, devem ser avaliadas: (i) a adoção de medidas de acordo com os princípios da proteção de dados desde a conceção e por defeito (*privacy by design* e *privacy by default*); (ii) a adequação dos níveis de segurança implementados; (iii) a aplicação de políticas de proteção de dados relevantes ao nível da administração da entidade em causa; e (iv) a existência e implementação de boas práticas de mercado.
- Outro fator a ter em conta será a existência ou ausência de antecedentes de incumprimentos imputáveis ao responsável, considerando ainda para o efeito o facto de se tratar ou não do mesmo tipo de incumprimento, bem como a reação do responsável face a incumprimentos anteriores.
- Por fim, assumem ainda relevância quaisquer outras circunstâncias agravantes ou atenuantes concretamente aplicáveis, tais como o lucro obtido em função do incumprimento em questão.

Através deste documento, o GT29 visa apoiar as autoridades de controlo no âmbito da sua tarefa de aplicação de coimas em caso de violação de dados pessoais, reforçando o facto de estarmos perante um cenário ainda em evolução e salientando a relevância atribuída à necessidade de cooperação entre autoridades nacionais de controlo, dando origem a jurisprudência em matéria de violação de dados pessoais ao abrigo do RGPD.

## 2. ORIENTAÇÕES SOBRE DECISÕES AUTOMATIZADAS E DEFINIÇÃO DE PERFIS

As Orientações sobre decisões automatizadas e definição de perfis ([Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, wp251](#)), que se encontram em consulta pública até 28 de novembro de 2017, procedem a uma análise exaustiva do âmbito de aplicação do artigo 22.º do RGPD, nos termos do qual os titulares dos dados têm o direito de não ficarem sujeitos a decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos nas respetivas esferas jurídicas ou que os afete significativamente de forma similar.

O GT29 aborda os diversos tipos de análise de perfil e requisitos associados, focando ainda o tratamento de dados pessoais de menores.

As Orientações procedem ainda a uma análise dos direitos gerais atribuídos aos titulares dos dados ao abrigo do RGPD, entre os quais se encontram: (i) o direito à informação, o qual implica a necessidade, por parte do responsável, de informar especificamente os titulares caso haja lugar a decisões automatizadas, incluindo a definição de perfis, fornecendo-lhes informações referentes aos termos e condições de tratamento, bem como aos potenciais impactos do mesmo; (ii) o direito de acesso, relativamente ao qual o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica, possibilitando ao titular o acesso direto aos respetivos dados (sempre que possível); e (iii) o direitos de retificação e apagamento dos dados, pois com a forte componente de previsão inerente à definição de perfis, o risco de imprecisão aumenta substancialmente.

Por forma a assegurar a transparência e rigor do tratamento realizado neste âmbito, os responsáveis pelo tratamento deverão implementar medidas de cariz técnico, tais como mecanismos de auditoria a algoritmos, e realizar avaliações regulares ao funcionamento dos sistemas.

Considerando as possíveis dificuldades de operacionalização, o GT29 avança com um conjunto de recomendações que as organizações poderão adotar por forma a garantir o cumprimento do RGPD, nesta matéria.

### 3. ORIENTAÇÕES SOBRE VIOLAÇÕES DE DADOS PESSOAIS

Neste documento ([Guidelines on Personal data breach notification under Regulation 2016/679, wp250](#)), que estará em consulta pública até 28 de novembro de 2017, o GT29 procede a uma análise da criação, ao abrigo do RGPD, da obrigação de notificação, por parte do responsável pelo tratamento, de violações de dados pessoais.

O GT29 recomenda aos responsáveis e subcontratantes a elaboração e adoção de planos de resposta a violações de dados, baseados em avaliações de risco, ficando desta forma aptos a detetar e controlar qualquer incidente de segurança de forma mais rápida e eficaz.

Na opinião do GT29, uma política de segurança eficaz tem precisamente por base a prevenção de violações e, caso estas ocorram, a capacidade de reação em tempo útil. Desta forma, tanto o responsável como os respetivos subcontratantes deverão implementar medidas técnicas e organizacionais apropriadas com vista a assegurar um nível adequado de segurança dos dados objeto de tratamento, tendo em conta o estado da arte e custos de implementação destas medidas, o âmbito, contexto e finalidades do tratamento em causa, bem como os riscos para os titulares dos dados.

As Orientações debruçam-se ainda sobre as situações de violações de dados pessoais que devem efetivamente ser objeto de notificação à autoridade de controlo e aos titulares dos dados, analisando diversos tipos de incidentes sob a perspetiva do risco para os direitos e liberdades dos titulares dos dados, bem como o impacto negativo inerente à violação (físico, material ou imaterial), sem prejuízo da necessidade de avaliação casuística.

Nestas Orientações, o GT29 procede também a uma análise dos critérios essenciais a ter em conta em sede de avaliação do risco inerente a uma violação de dados, sendo eles:

- O tipo de violação de dados pessoais
- A natureza, sensibilidade e volume dos dados afetados
- A facilidade com que os titulares dos dados em causa poderão ser identificados
- A gravidade e impacto temporal das consequências da violação para os titulares dos dados
- As características dos titulares dos dados (nomeadamente no que diz respeito a crianças)
- O número de indivíduos afetados pela violação
- Determinadas características especiais do responsável pelo tratamento (tal como o facto de se tratar de uma entidade que procede sobretudo ao tratamento de categorias especiais de dados).

Por último, o GT29 salienta o dever de manutenção de registos atualizados de quaisquer violações de dados, independentemente da obrigatoriedade da respetiva notificação à autoridade de controlo, aconselhando os responsáveis pelo tratamento a documentar todas as decisões internas e medidas adotadas em resposta a cada violação e, em especial, a justificação para a não notificação de determinadas violações, por forma a salvaguardar a sua posição perante a autoridade de controlo competente.

Todas estas e futuras orientações (tais como as aplicáveis ao consentimento que serão, de acordo com o GT29, emitidas ainda em 2017), deverão ser tidas em consideração pelas organizações no âmbito do seu processo de implementação do RGPD.