26 de abril de 2017

Magda Cocco | mpc@vda.pt
Inês Antas de Barros | iab@vda.pt
Isabel Ornelas | igo@vda.pt
Maria de Lurdes Gonçalves | mlg@vda.pt
Nádia Crujeira da Costa | ncc@vda.pt

PRIVACIDADE, PROTEÇÃO DE DADOS & CIBERSEGURANÇA

ORIENTAÇÕES DO GRUPO DE TRABALHO DO ARTIGO 29 SOBRE O REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS

De forma a esclarecer algumas das novas obrigações previstas no Regulamento Geral sobre a Proteção de Dados ("RGPD") aplicável a partir de 25 de maio de 2018, o Grupo de Trabalho do Artigo 29.º ("GT29") - órgão europeu independente com funções consultivas em matéria de proteção de dados - emitiu recentemente **Orientações sobre as Avaliações de Impacto sobre a Proteção de Dados (Data Protection Impact Assessment – "DPIAs")**, que estarão em consulta pública até 23 de maio de 2017.

Quando é obrigatória a realização de um DPIA?

O RGPD prevê que o DPIA (avaliação de impacto sobre a proteção de dados) deve ser realizado quando o tratamento de dados "for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares". O RGPD estabelece uma lista de situações em que o DPIA é obrigatório, esclarecendo, porém, que tal lista é meramente exemplificativa e que, em caso de dúvida, as entidades responsáveis devem realizar o DPIA. O GT29 avança ainda com alguns fatores que levam à necessidade de realização de um DPIA, tais como o tratamento de dados de titulares considerados vulneráveis (menores e trabalhadores), a existência de transferências diárias de dados para fora da União Europeia, entre outros.

Caso o responsável conclua que não é necessário realizar um DPIA, deverá documentar tal análise e conclusão.

Quando e como deve ser realizado o DPIA?

O DPIA, da responsabilidade da entidade responsável (que pode ser coadjuvada por terceiros), deve ser realizado com a antecedência necessária para ser possível acautelar e implementar as recomendações nele previstas. O GT29 recomenda que os DPIAs sejam revistos a cada três anos, exceto nas situações em que o tratamento seja objeto de alterações, caso em que a reavaliação deve ser efetuada em momento prévio à introdução de tais alterações.

Quais os tratamentos abrangidos?

O GT29 esclarece que apenas estão sujeitos à obrigação de realização de um DPIA os tratamentos de dados iniciados após 25 de maio de 2018. Relativamente aos tratamentos iniciados em data anterior, será obrigatório caso sejam inseridas alterações ao tratamento dos dados após a aplicação do RGPD.

Quando há lugar a consulta prévia?

O RGPD prevê a obrigação de consulta prévia à Autoridade de Controlo (CNPD) quando o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável para atenuar tal risco. O GT29 esclarece que a lei nacional pode prever outras situações em que a consulta é obrigatória, ainda que tal elevado risco não exista.

O GT29 aprovou ainda, e depois de um período de consulta pública, as versões finais das orientações relativas à nomeação de um **Data Protection Officer (DPO)**, em português o "Encarregado de Proteção de Dados", ao **direito à portabilidade dos dados pessoais** (i.e. o direito que garante ao titular dos dados a possibilidade, verificadas certas condições, de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, assim como o direito de transmitir esses dados a outro responsável pelo tratamento) e à identificação da **autoridade de controlo principal**.

São introduzidas, nas versões finais das orientações, algumas alterações das quais destacamos as seguintes:

1. Orientações sobre a Nomeação de um DPO:

- A nomeação do DPO, quer seja obrigatória quer seja voluntária, é efetuada para todas as atividades de tratamento de dados levadas a cabo pelo responsável pelo tratamento ou pela entidade subcontratante;
- É recomendado que o DPO esteja localizado na União Europeia, ainda que o responsável pelo tratamento ou a entidade subcontratante não o estejam;
- Ainda que o DPO esteja vinculado a obrigações de segredo e confidencialidade, poderá sempre solicitar orientações sobre os tratamentos de dados levados a cabo pelos responsáveis, às autoridades de controlo;
- Numa organização apenas poderá existir um DPO, ainda que possa ser suportado por uma equipa;
- Senior Managers, tais como o Diretor de Recursos Humanos, de Marketing ou de IT não podem exercer funções de DPO.

2. Orientações sobre o direito à portabilidade dos dados:

- Perante um pedido de portabilidade, os responsáveis pelo tratamento que recebam tal pedido não são responsáveis pelo tratamento de dados ulterior efetuado pelo titular dos dados ou pela organização que os receba;
- As entidades subcontratantes devem prestar auxílio aos responsáveis pelo tratamento na resposta a um pedido de portabilidade de dados;
- As organizações que recebam os dados pessoais não estão obrigadas a aceitar e a tratar os dados pessoais recebidos, na sequência de um pedido de portabilidade de dados pessoais;
- Os dados relativos à atividade dos titulares dos dados (tais como, logs e histórico de pesquisa) estão abrangidos pelo direito à portabilidade dos dados pessoais;
- Os responsáveis pelo tratamento devem explorar duas formas complementares de assegurar a portabilidade dos dados: (i) transmissão direta dos dados e (ii) utilização de uma ferramenta automática de extração dos dados. A escolha deve ser feita caso a caso.

3. ORIENTAÇÕES SOBRE A AUTORIDADE DE CONTROLO PRINCIPAL:

- No caso de corresponsabilidade de entidades localizadas em diferentes Estados Membros, os responsáveis pelo tratamento devem determinar, de forma transparente, as respetivas responsabilidades e, de forma a beneficiar do mecanismo de balcão único ("one stop shop"), identificar o estabelecimento que tem o poder de determinar os termos do tratamento de dados;
- O mecanismo de balcão único pode ainda beneficiar entidades subcontratantes que tenham estabelecimentos em diferentes Estados Membros;
- Sem prejuízo do ponto anterior, quando, na mesma operação de tratamento, estejam envolvidos diferentes responsáveis pelo tratamento e entidades subcontratantes localizadas em diferentes Estados Membros, a Autoridade de Controlo principal será a autoridade onde está localizado o estabelecimento principal do responsável pelo tratamento, o que significa que a entidade subcontratante poderá ter que lidar com diferentes autoridades de controlo.