Momentum

Contencioso e Arbitragem

10 de novembro de 2014

# O NOVO REGULAMENTO GERAL DA UNIÃO EUROPEIA RELATIVO À PROTEÇÃO DE DADOS: UMA PERSPETIVA EMPRESARIAL

Em janeiro de 2012, a Comissão Europeia apresentou uma proposta de reforma do quadro legal europeu em matéria de proteção de dados pessoais, onde se inclui a proposta de um regulamento[1] geral, prevendo-se que o processo de aprovação esteja finalizado na primeira metade de 2015.

De uma perspetiva empresarial, segue uma breve resenha de algumas das mais relevantes alterações previstas na proposta de regulamento.

De um lado, a uniformização do quadro legal para os 28 Estados-membros, levará a que uma empresa que opere em diversos Estados-Membros não tenha custos com a adaptação à legislação em vigor em cada um deles, o que, a par do princípio *one-stop-shop*[2] – segundo o qual uma empresa apenas tem de lidar com a autoridade de supervisão do país do estabelecimento principal –, levará a uma redução de custos administrativos.

[1] No presente texto faremos apenas referência à proposta de regulamento. Todavia, o quadro jurídico proposto inclui ainda a «*diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados*».

[2] Todavia, um particular ou uma associação para defesa do interesse público podem apresentar queixas numa autoridade de supervisão distinta da do estabelecimento principal.

Igual redução se verificará com a eliminação das notificações a autoridades de supervisão, na sua configuração atual, e redução de situações em que é necessária autorização prévia.

Do outro lado, encontra-se uma acrescida responsabilização dos responsáveis pelo tratamento, que torna aconselhável a realização de auditorias ainda antes da entrada em vigor do regulamento. O responsável pelo tratamento deve estar sempre apto a demonstrar que adotou todas as medidas técnicas e organizacionais necessárias, devendo as políticas de *compliance* ser revistas a cada dois anos. Além do mais, devem ser feitas avaliações de impacto, deve ser mantida a documentação necessária, entre outros procedimentos que podem levar a um aumento de custos, e cuja demonstração deve poder ser feita a qualquer momento.

As empresas – que tratem dados de 5.000 ou mais titulares num período consecutivo de doze meses, tratem categorias especiais de dados ou cuja atividade implique um acompanhamento regular dos titulares dos dados – devem ter um delegado de proteção de dados, responsável por assegurar o cumprimento do quadro legal.

Além do mais, de acordo com os conceitos de «*privacy by design*» e «*privacy by defaut*», o cumprimento do quadro legal nesta matéria deve ser pensado logo aquando da escolha dos meios para proceder ao tratamento, que devem garantir, por defeito, que apenas são tratados dados para a finalidade em causa, que a recolha não é excessiva, e que o tempo de conservação está de acordo com a lei.

Os sistemas dos responsáveis pelo tratamento devem estar aptos a assinalar qualquer falha de segurança de dados, que deve ser notificada à autoridade competente e aos afetados no prazo de 24 horas. Este facto, associado às

novas regras quanto à obtenção de consentimento para o tratamento de dados junto do titular, ao direito ao esquecimento e ao direito à portabilidade dos dados, entre outras, leva a que muitos dos responsáveis pelo tratamento tenham de reconfigurar os seus sistemas e procedimentos.

Outro ponto de grande importância é a aplicação extraterritorial do regulamento, já que se aplicará a todas as empresas que operem na União Europeia, mesmo que aí não tenham o seu estabelecimento. Em alguns casos, empresas situadas fora da União, necessitam de designar um representante, que responde perante a autoridade de supervisão.

Por fim, cabe-nos referir que as autoridades de supervisão terão um leque mais alargado de competências. Por exemplo, poderão aplicar sanções administrativas até 5% do volume de negócios mundial anual de uma empresa, ou até € 100 000 000 de acordo com o valor mais elevado.

As regras elencadas são apenas algumas das constantes da proposta de regulamento, e devem ser tidas em conta pelos responsáveis pelo tratamento de dados, evitando, entre outras consequências, eventuais danos reputacionais causados pelo incumprimento de regras numa área considerada sensível, e a aplicação de coimas bastante elevadas.

Marta Salgado Areias

mva@servulo.com





Rua Garrett, n.º 64 1200-204 Lisboa - Portugal Tel: (+351) 21 093 30 00 Fax: (+351) 21 093 30 01/02
geral@servulo.com www.servulo.com