



BRANDS' ADVOCATUS

O Novo Regulamento da E-Privacy

Por JOÃO SANTIAGO SILVA

Associado da CMS
Rui Pena & Arnaut

O que é a ePrivacy?

A ePrivacy representa fundamentalmente o respeito pela vida privada, a garantia da confidencialidade e a proteção de dados pessoais no âmbito das comunicações eletrónicas.

Mas por que razão se ouve falar tanto de ePrivacy?

Em grande medida, porque o utilizador comum, bem como as próprias empresas, estão cada vez mais dependentes de novos serviços disponibilizados através da Internet, que permitem comunicações interpessoais, tais como serviços VoIP (Voice Over Internet Protocol), mensagens instantâneas e/ou de correio eletrónico.

É por isso importante que as empresas se comecem a preparar para a substituição da atual Diretiva pelo novo Regulamento de ePrivacy (doravante, Regulamento) que se prevê entrar em vigor já em 2019.

Consequência da intenção de aumentar a confiança e a segurança na prestação de serviços digitais, o Regulamento visa elevar a proteção dos dados pessoais e da privacidade dos utilizadores finais no âmbito dos serviços de comunicações eletrónicas.

O que muda com o novo Regulamento?

O Regulamento de ePrivacy tem como principais objetivos (i) garantir um alinhamento com o RGPD, (ii) assegurar um maior nível de proteção aos utilizadores de serviços de comunicações eletrónicas e (iii) garantir a harmonização legal no EEE.

Para tal, o Regulamento de ePrivacy introduz, entre outras, várias novidades:

Reforço da confidencialidade, pelo que qualquer interferência através da instalação de dispositivos de escuta, armazenamento, controlo, digitalização ou outras formas de interceção, vigilância ou tratamento de dados de comunicações eletrónicas é proibida sem o consentimento dos utilizadores finais, salvo em casos excecionais.

O âmbito de aplicação material é alargado, já que passa a abranger serviços anteriormente excluídos da aplicação da antiga Diretiva, como sejam serviços over the top (OTT), usualmente prestados através de

uma ligação à rede de Internet de uma operadora de telecomunicações (e.g. WhatsApp, Facebook ou Gmail).

Deste modo, serviços de chamadas e/ou mensagens por via telefónica, a navegação na Internet, o envio e receção de e-mails e/ou outros serviços que permitam comunicações interpessoais entre utilizadores (e.g. plataformas de jogos online) serão afetados pelo impacto legal deste Regulamento.

Verifica-se um reforço da não discriminação entre pessoas singulares e pessoas coletivas, na medida em que as disposições do Regulamento visam garantir o mesmo nível de proteção a ambas. Tal resulta do entendimento de as comunicações eletrónicas poderem conter informações suscetíveis de serem confidenciais, designadamente segredos comerciais ou outras informações sensíveis e com valor económico.

Procede-se ao reforço da proteção dos metadados, pelo que se visa assegurar a confidencialidade não só do conteúdo propriamente dito das comunicações eletrónicas mas também dos referidos metadados que, não deixando de ser qualificados como dados pessoais, deverão ser anonimizados ou eliminados caso o utilizador final não preste o respetivo consentimento.

Há um reforço da proteção contra comunicações não solicitadas, tendo em consideração que, em alguns casos, poderá ser necessário recolher o consentimento prévio de pessoas coletivas nos termos do RGPD.

Realiza-se uma revisão das regras em matéria de cookies, na medida em que a proposta visa melhorar a navegação dos utilizadores finais na Internet. Para o efeito, a Comissão Europeia esclarece que não é necessário facultar o consentimento para a utilização de cookies não intrusivos.

Por fim, agrava-se o regime sancionatório, nomeadamente pela aplicação coimas que podem chegar a 20 milhões de euros ou 4% da faturação do volume de negócio anual.

Como é que as empresas se devem preparar?

As organizações devem proceder a uma abordagem holística e conjunta com o RGPD, de modo a identificar as obrigações específicas impostas pelo Regulamento.

Neste contexto, devem proceder (i) a um levantamento da sua situação atual, (ii) à análise das situações de não conformidade que sejam identificadas (gap analysis) e (iii) à implementação de medidas que visem mitigar o risco das situações identificadas e que permitam criar um ambiente de compliance com o Regulamento.

Por fim, ainda se aconselha que as organizações encarem este desafio como uma oportunidade para melhorar os seus produtos e serviços, bem como a sua eficiência e competitividade no mercado onde se inserem. ●