



PRIVACIDADE E DADOS PESSOAIS | Novo Pacote Legislativo de Protecção de Dados Pessoais

Ontem, dia 25 de Janeiro de 2012, a Comissão Europeia publicou a versão final da proposta de Pacote Legislativo de Protecção de Dados Pessoais, que inclui o Regulamento de Protecção de Dados Pessoais (“Regulamento”), que alterará a Directiva 95/46/CE. O Regulamento entrará, agora, em processo legislativo, sendo expectável que leve dois anos a ser concluído.

O Pacote Legislativo de Protecção de Dados Pessoais inclui ainda uma Directiva relativa ao tratamento de dados para efeitos de justiça criminal, assim como uma Comunicação e Relatório relativos à cooperação judicial e policial.

Destaca-se, do Pacote Legislativo de Protecção de Dados, Pessoais o Regulamento, visto consagrar uma alteração profunda às regras de protecção de dados ainda vigentes, de entre as quais se destacam as seguintes:

- **Maior responsabilização do responsável pelo tratamento e aplicação, às entidades subcontratadas, de muitas das obrigações que são actualmente apenas impostas aos responsáveis pelo tratamento de dados**

O Regulamento estabelece, em relação a alguns aspectos, uma equiparação entre o responsável e o subcontratado, prevendo um conjunto de obrigações que são aplicáveis a ambos.

Seguindo uma lógica de maior responsabilização, o Regulamento inclui uma descrição detalhada das obrigações do responsável em assegurar o cumprimento do Regulamento, através, nomeadamente, da adopção de políticas internas e de mecanismos para assegurar tal cumprimento. O Regulamento vai mais longe e consagra, explicitamente, o princípio da *privacy by design*, prevendo, em particular, a obrigação do responsável levar a cabo um *privacy impact assessment* previamente a uma operação de tratamento de dados considerada de risco.

O Regulamento clarifica a posição do subcontratado, adicionando alguns elementos novos, como sendo o facto de, se o subcontratado tratar dados para além das instruções do responsável, passará a ser considerado um co-responsável.

O responsável e o subcontratado passam a estar obrigados a manter toda a documentação relativa ao tratamento de dados pessoais, devendo, quando solicitado, cooperar com as autoridades nacionais de protecção de dados.

- **Adopção do consentimento explícito (*Opt-in*) como regra**

O Regulamento clarifica as condições em que o consentimento é considerado válido e, como tal, fundamento legal para o tratamento de dados. Em particular, estabelece-se que cabe ao responsável obter e demonstrar que o titular deu o seu consentimento (livre, expresso e explícito) e que, caso o consentimento seja dado por escrito, este deverá estar devidamente destacado dos outros aspectos regulados no documento.



PRIVACIDADE E DADOS PESSOAIS | Novo Pacote Legislativo de Protecção de Dados Pessoais

- **Reforço das obrigações de informação aos titulares dos dados**

O Regulamento introduz a obrigação dos responsáveis de disponibilizarem informação transparente e facilmente acessível ao titular dos dados, consagrando-se o direito de informação dos titulares em relação aos destinatários dos dados - quer estes destinatários sejam co-responsáveis, terceiros ou subcontratados.

Quanto ao conteúdo da informação, para além da informação já prevista na Directiva 95/46/CE, o responsável deverá passar a prestar informação adicional, como sendo o prazo de conservação dos dados e o direito de apresentação de reclamações.

- **Implementação do “direito ao esquecimento” (*the right to be forgotten*)**

O Regulamento introduz um novo direito – o direito ao esquecimento - estabelecendo que, perante um pedido de eliminação de dados, o responsável deverá adoptar mecanismos que assegurem que todos os dados foram efectivamente eliminados.

Em particular, e quando o responsável tenha, de alguma forma, tornado , os dados públicos ou comunicado tais dados a terceiros, deverá eliminar os links e cópias de tais dados, assegurando que o mesmo é efectuado pelos terceiros a quem comunicou os dados.

- **Obrigaçã de notificação de *data breaches***

O Regulamento dá um enfoque especial ao tema da segurança, prevendo uma responsabilidade conjunta do responsável e subcontratado em adoptar as medidas de segurança necessárias para proteger os dados contra acessos indevidos.

Consagra-se a obrigação de notificação de *data breaches* (violações de dados pessoais), prevendo-se, em termos gerais, que a notificação deve ser remetida à autoridade nacional de protecção de dados no prazo máximo de 24 horas, devendo conter informação sobre o tipo de incidente, consequências, medidas adoptadas e contactos.

Caso o incidente possa afectar negativamente a privacidade do titular dos dados, o responsável deverá também notificar os titulares dos dados da ocorrência de tal incidente.

- **Obrigaçã de nomeaçã de um *Data Protection Officer***

Os responsáveis e subcontratados passam a estar obrigados a nomear um *data privacy officer* quando o tratamento de dados seja efectuado (i) por uma autoridade ou organismo públicos; (ii) por uma empresa com 250 ou mais trabalhadores; ou (iii) por uma empresa cuja actividade principal consista no tratamento de dados pessoais.

O Regulamento estabelece as funções mínimas do *data privacy officer*. A saber (a título exemplificativo):

- | | |
|--|--|
| (i) informar e aconselhar o responsável/subcontratado relativamente às suas responsabilidades; | (iv) assegurar que o responsável/subcontratado mantém a documentação requerida pelo Regulamento; |
| (ii) monitorizar a implementação e aplicação de políticas internas; | (v) . monitorizar e acompanhar as notificações de <i>data breaches</i> ; |
| (iii) monitorizar a implementação e aplicação do Regulamento; | (vi) monitorizar a performance dos <i>data protection impact assessments</i> . |

PRIVACIDADE E DADOS PESSOAIS | Novo Pacote Legislativo de Protecção de Dados Pessoais

- ***Data protection impact assessment* e autorização prévia**

Quanto às formalidades de notificação, o Regulamento simplifica bastante os procedimentos, limitando a obrigação de consulta e obtenção de autorização prévia a situações específicas.

A este respeito refira-se que o Regulamento introduz a obrigação dos responsáveis e subcontratados levarem a cabo uma avaliação do impacto ao nível da protecção de dados, previamente a qualquer operação de tratamento de dados considerada de risco. Serão, entre outras, consideradas de risco as operações que envolvam o tratamento de dados de saúde ou dados genéticos.

- **Reconhecimento das *Binding Corporate Rules***

Uma das grandes alterações em matéria de transferências internacionais de dados é o reconhecimento expresso das *Binding Corporate Rules* (regras de protecção de dados pessoais acordadas e vinculativas no seio de um grupo empresarial) como fundamento para a transferência de dados para países terceiros.

Estabelece-se ainda a possibilidade de celebração de contratos (que não as *standard contractual clauses* aprovadas pela Comissão Europeia), estando, no entanto e em tal caso, a transferência sujeita a autorização prévia da autoridade nacional de protecção de dados.

- **Aumento dos valores das coimas**

O Regulamento prevê um conjunto de sanções aplicáveis em caso de não cumprimento das suas disposições, estabelecendo a possibilidade de aplicação de coimas até 1 000 000 € ou, em caso de pessoas colectivas, até ao montante correspondente a 2% do volume anual de negócios a nível mundial.

É inegável o acentuado impacto que o novo Regulamento de Protecção de Dados Pessoais terá - quando entrar em vigor - na organização das empresas, levando a que as mesmas tenham que, necessariamente, alterar os seus procedimentos internos em matéria de *privacy compliance*.