GUIA

Proteção de dados: Sete medidas que as empresas devem adotar

João D'Espiney

26.05.2017 / 17:30

O novo regulamento europeu de proteção de dados pessoais vai entrar em vigor precisamente daqui a um ano. Saiba o que as empresas devem fazer.

A 25 de maio de 2018, ou seja, daqui a precisamente um ano, vai entrar em vigor o novo regulamento geral de proteção de dados (RGPD) pessoais.

A grande maioria das organizações em Portugal está ainda muito longe de estar preparada para as exigências decorrentes do novo regulamento. Esta quinta-feira de manhã, à mesma hora que eram apresentados os resultados de um inquérito coordenado pelo IAPMEI a cerca de 1600 empresas, a sociedade de advogados Macedo Vitorino & Associados realizou uma conferência para dar a conhecer o impacto das principais alterações no dia-a-dia das organizações.

Recorde-se que o novo regulamento coloca o ónus de responsabilidade do tratamento e da conformidade dos dados pessoas nas organizações, públicas e privadas – até agora da competência da Comissão Nacional de Proteção de Dados (CNPD).

O RGPD prevê ainda novas obrigações com um impacto considerável nas suas operações, nomeadamente um registo com todas as operações de dados pessoais, que até aqui não era obrigatório.

Outra das grandes novidades é o agravamento substancial das multas pelo incumprimento do novo regulamento, que poderão ir até aos 20 milhões de euros.

Cláudia Fernandes Martins, jurista deste escritório de advogados elaborou um guia com as sete medidas que as empresas deverão adotar para estarem em conformidade com o novo RGPD.

1 – Criar um sistema de registo de dados
O objetivo é identificar os dados que são recolhidos, de onde vêm, como, porquê e com quem são partilhados.

A ideia-chave é "mapear" os dados utilizados pela empresa e depois agrupá-los em conjuntos identificáveis, funcionais e com riscos similares ao nível da sua proteção e conservação.

É preciso ter em conta as categorias de dados, a finalidade de tratamento, o prazo de conservação e o âmbito geográfico do tratamento.

2 – Rever a política de privacidade, procedimentos e documentação e demonstrar que está a cumprir o RGPD
Em causa está a necessidade de verificar se o consentimento dos titulares dos dados se manterá válido e se se poderá recorrer a outros fundamentos. O consentimento deve ser livre, específico, informado e corresponder a uma clara ação afirmativa do titular dos dados (oral ou escrita).

Em caso de tratamento de dados sensíveis ou transferência de dados para fora da União Europeia, o consentimento tem de ser explícito. O silêncio, opções pré-validadas ou a omissão do titular dos dados não constituem consentimento.

Quando o tratamento for realizado com fundamento em consentimento, deverá ser capaz de demonstrar que o titular deu o seu consentimento. Este requisito poderá ser particularmente difícil de demonstrar em determinados casos, o que poderá exigir uma abordagem mais proativa das empresas.

O RGPD será diretamente aplicável aos subcontratantes, que passam a estar sujeitos a obrigações mais detalhadas e poderão ficar obrigados ao pagamento de indemnização em caso de ocorrência de prejuízos. Nesse sentido, reveja todos os contratos com subcontratantes e, se for necessário, reconsidere a sua posição.

O RGPD será diretamente aplicável aos subcontratantes, que passam a estar sujeitos a obrigações mais detalhadas e poderão ficar obrigados ao pagamento de indemnização em caso de ocorrência de prejuízos. Nesse sentido, reveja todos os contratos com subcontratantes e, se for necessário, reconsidere a sua posição.

O novo regulamento impõe que se crie e mantenha um registo das atividades de tratamento se: tiver mais de 250 trabalhadores; o tratamento de dados for suscetível de implicar um risco para os direitos do titular; o tratamento não for ocasional; ou se os tratamentos incluam dados sensíveis ou dados relativos a condenações penais e infrações.

Os registos devem ser escritos e incluir informação sobre os tratamentos de dados efetuados, incluindo os contactos do responsável pelo tratamento e do encarregado de proteção de dados, as finalidades de tratamento, as categorias de dados, os seus destinatários, transferências internacionais de dados e medidas de segurança.

3 – Ter em conta os novos direitos dos titulares dos dados
As organizações vão ter de assegurar que conseguem cumprir com dois direitos fundamentais: "o direito de portabilidade" e o "direito a ser esquecido".

O "direito de portabilidade" dos dados reforça o já existente direito de acesso dos titulares aos seus dados pessoais através de um pedido de acesso. Este novo direito permite ao titular dos dados pedir e receber os seus dados pessoais, que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso correntes e de leitura automática.

O titular dos dados terá ainda o direito de transmitir esses dados, de forma gratuita, a outro responsável pelo tratamento e sem que o primeiro responsável a quem foram fornecidos o possa impedir.

Na prática, isto significa que poderá ter de implementar determinadas medidas técnicas, como permitir o *download* direto dos dados pelos titulares ou disponibilizar um interface de programação de aplicações.

O "direito a ser esquecido" ou "direito ao apagamento" significa que os titulares dos dados têm direito a obter do responsável pelo tratamento o apagamento dos seus dados pessoais e a abstenção de qualquer disseminação futura desses dados, incluindo dados disponíveis ou processados em formato eletrónico.

Este direito tem, no entanto, algumas exceções, como por exemplo para o cumprimento de uma obrigação legal ou execução de uma tarefa determinada pelo interesse público, por motivos de saúde pública, para fins de arquivo de interesse público, para fins estatísticos e para fins de investigação científica ou histórica.

4 – Assegurar que os recursos humanos estão conscientes das implicações do RGPD e têm formação sobre as novas regras

Deverá verificar se cumpre os requisitos para ser obrigatório designar um Encarregado de Proteção de Dados (EPD) e de que forma esta função se enquadrará no seio da organização.

Para isso poderá ser necessário criar uma função específica para desempenhar a função de EPD, designar um único EPD ou um EPD por cada empresa ou jurisdição do grupo.

A designação de um EPD, quando seja obrigatória aplica-se aos responsáveis pelo tratamento e subcontratantes. Quando o responsável pelo tratamento preencha os requisitos de designação obrigatória, o subcontratante não será obrigado a designar um EPD, se ele próprio não preencher tais requisitos.

Mesmo quando não é obrigatória, poderá ser aconselhável designar um EPD por forma a centralizar as questões de proteção de dados e facilitar o cumprimento do novo regulamento.

O RGPD requer a designação de um EPD em três casos específicos: quando o tratamento for efetuado por um organismo público (exceto tribunais); quando as atividades principais do responsável ou subcontratante consistam em operações de tratamento que exijam um controlo sistemático e regular dos titulares dos dados em grande escala (serviços de telecomunicações, bancos, seguradoras); ou quando as atividades principais do responsável ou subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados (genéticos, biométricos, de saúde) ou dados pessoais relacionados com condenações penais e infrações.

5 – Adotar medidas e políticas internas que cumpram os requisitos de proteção "desde a conceção" e proteção "por defeito"

A "proteção desde a conceção" requer que o responsável pelo tratamento de dados aplique, quer no momento de definição dos meios de tratamento quer no momento do próprio tratamento, medidas técnicas e organizativas adequadas.

Estas medidas podem incluir: minimização do tratamento de dados; pseudonimização de dados pessoais o mais cedo possível; adoção de medida de transparência relativas às funções e ao tratamento de dados pessoais; possibilidade de o titular dos dados controlar o tratamento de dados; e possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança.

A "proteção por defeito" requer que o responsável pelo tratamento implemente medidas técnicas e organizativas adequadas destinadas a assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento (incluindo a quantidade de dados pessoais recolhidos, a extensão do seu tratamento, o seu prazo de conservação e a sua acessibilidade).

6 – Rever e atualizar as medidas de segurança do tratamento
O novo regulamento prevê a aplicação das seguintes medidas técnicas e organizativas: A começar pela pseudonimização e cifragem dos dados pessoais e pela capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento.

A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico e ter um processo para testar, apreciar e avaliar regularmente a eficácia das medidas adotadas para garantir a segurança do tratamento são outras das medidas previstas.

Estas medidas não são obrigatórias em todos os casos. Cada empresa tem o direito de optar por outras. Contudo, se nenhuma medida adequada for adotada, poderá vir a revelar-se difícil justificar uma violação de dados por uma falha do sistema de segurança, o que aumenta a probabilidade de a empresa vir a ser sancionada no pagamento de coimas.

O regulamento prevê ainda a possibilidade de criar um procedimento de notificação em caso de violação de dados pessoais. Nesses casos, o responsável pelo tratamento de dados deverá notificar a Comissão Nacional de Proteção de Dados (CNPD) até 72 horas depois de ter conhecimento e informar o titular dos dados sem demora injustificada.

7 – Rever o impacto sobre as transferências transfronteiriças de dados
O novo regulamento reforça as atuais regras sobre transferências internacionais de dados, que são permitidas desde que apresentem garantias adequadas.

Além das soluções existentes, como as "cláusulas contratuais-tipo" e o consentimento do titular, o RGPD prevê novas soluções.

As "cláusulas contratuais-tipo" deixam de requerer a autorização prévia da CNPD, ainda que a transferência envolva dados sensíveis. Não é de excluir, porém, que a CNPD possa vir a exigir uma notificação prévia para essas operações de tratamento.

As regras vinculativas aplicáveis às empresas são outra das soluções ao abrigo da qual as entidades de um grupo empresarial se obrigam a realizar entre si transferências de dados.

Ao contrário das "cláusulas contratuais-tipo", que têm a desvantagem de nã serem aplicáveis entre entidades subcontratantes, as regras vinculativas estarão disponíveis tanto para responsáveis pelo tratamento como para subcontratantes.

As jurisdições "permitidas", isto é, os países para os quais é permitido transferir dados pessoais, por ser "essencialmente equivalente" ao RGPD é outra das soluções.

O "Escudo de Proteção da Privacidade" de dados UE-EUA, que vem substituir o anterior acordo, invalidado pelo Tribunal de Justiça da UE, é outra das opções.

As transferências de dados não repetitivas e que apenas digam respeito a um número limitado de titulares de dados poderão ser, em situações excecionais, justificadas mediante a notificação à autoridade de supervisão e prestação de informação ao titular dos dados.