REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS

AS SETE MEDIDAS QUE AS EMPRESAS DEVEM ADOTAR

MACEDO VITORINO & ASSOCIADOS
Sociedade de Advogados, RL

INTRODUÇÃO

O Regulamento Geral sobre a Proteção de Dados ("RGPD") promete trazer significativas alterações em matéria de proteção de dados (as maiores dos últimos vinte anos) desde a Diretiva n.º 95/46/CE, que foi transposta pela Lei n.º 67/98, de 26 de outubro.

O RGPD será diretamente aplicável em todos os Estados Membros da União Europeia ("UE") a partir de 25 de maio de 2018. O novo regulamento terá ainda um âmbito de aplicação global, na medida em que empresas sedeadas fora da UE, que disponibilizem bens ou serviços na UE, poderão ficar sujeitas ao RGPD.

O risco de multas até 4% do volume de negócios anual, a nível mundial, ou de 20 milhões de euros constitui um incentivo mais do que suficiente para que as empresas cumpram o RGPD.

O RGPD não impede, todavia, que a lei portuguesa possa estabelecer requisitos mais específicos, nomeadamente em matéria de tratamento de dados sensíveis (e.g., dados genéticos, dados biométricos e dados referentes a saúde) e de dados pessoais dos trabalhadores no contexto laboral (para efeitos, entre outros, de recrutamento, execução de contrato de trabalho, cessação da relação de trabalho), normas que se aplicarão conjuntamente com o RGPD.

A aplicação conjunta do RGPD e da lei portuguesa será relevante nos casos em que as empresas recolham e tratem dados de indivíduos portugueses e/ou a autoridade de supervisão portuguesa (a Comissão Nacional de Proteção de Dados – "CNPD") atue na qualidade de autoridade principal pelo facto de o estabelecimento principal ou o estabelecimento único do responsável pelo tratamento ou subcontratante se encontrar localizado em Portugal.

Os titulares de dados, residentes em Portugal, terão o direito de apresentar reclamações junto da CNPD. Em processos apresentados contra o responsável pelo tratamento ou subcontratante, o reclamante terá direito a recorrer aos tribunais portugueses se as empresas ou a residência do responsável pelo tratamento ou subcontratante se encontrarem localizados em Portugal.

Apesar de, em termos gerais, as regras fundamentais continuem a ser as mesmas, existem importantes alterações com impacto no dia-a-dia das empresas e para as quais deverão estar alerta e preparar-se com a devida antecedência.

O objetivo desta publicação é o de definir um plano com sete medidas a adotar pelas empresas para cumprirem o RGPD. As empresas também deveriam aproveitar esta oportunidade para melhorarem a sua forma de lidar com os dados pessoais. A contagem decrescente para 2018 já começou…

1. Crie um sistema de registo de dados.

Crie um sistema de registo de dados por forma a identificar que dados são recolhidos, de onde vêm, como, porquê e com quem são partilhados.

Um "sistema de registo de dados" pode ser definido como um conjunto de dados determinados e geridos de forma unitária (e.g. base de dados de contatos de clientes, dados de saúde de trabalhadores). A ideia-chave é "mapear" os dados utilizados pela sua empresa e depois agrupá-los em conjuntos identificáveis, funcionais e com riscos similares ao nível da sua proteção e conservação, tendo em conta:

- As categorias de dados (incluindo dados sensíveis);
- A finalidade de tratamento;
- O prazo de conservação;
- O âmbito geográfico do tratamento, etc..

Para o efeito, tenha em conta que a lei portuguesa poderá estabelecer requisitos mais específicos quanto a certas categorias de dados (e.g. dados sensíveis).

Tenha a certeza que a sua análise inclui todos os dados pessoais relacionados com a sua empresa. Pondere realizar uma auditoria aos dados pessoais.

Esta não é necessariamente uma tarefa com custos elevados, pois é provável que já tenha recursos disponíveis na sua empresa que possam ser utilizados.

Poderá solicitar a cada departamento e a cada estabelecimento localizado em cada país onde esteja presente para especificar:

- As categorias de dados, em particular realiza tratamento de dados sensíveis;
- As finalidades de tratamento;
- O prazo de conservação de cada categoria de dados;
- Onde se encontram guardados os dados, etc..

Poderá utilizar documentação de prévias auditorias, medidas técnicas de registo e gestão, listas de software, etc.. Isto permitir-lhe-á compreender que dados pessoais são tratados e como poderá geri-los e protegê-los no âmbito da sua organização.

2. Reveja a sua política de privacidade, procedimentos e documentação.

Reveja a sua política de privacidade e se o consentimento dos titulares dos dados se manterá válido e se poderá recorrer a outros fundamentos.

O consentimento do titular dos dados é apenas um dos fundamentos legítimos para o tratamento de dados, mas podem existir outros fundamentos (e.g. se o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte ou para diligências pré-contratuais a pedido do titular dos dados).

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 UE, o consentimento tem que 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. Isto poderá exigir uma abordagem mais proativa das empresas no seu dia-a-dia.

Reveja os contratos com subcontratantes e, se necessário, reconsidere a sua posição.

O RGDP 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.

Se atua enquanto responsável pelo tratamento (i.e., se determina a finalidade e os meios de tratamento dos dados), deverá atualizar o seu acordo-quadro de forma a incorporar a nova terminologia e obrigações dos subcontratantes impostas pelo RGPD e verificar se será necessário atualizar os contratos com os subcontratantes atuais.

Se atua enquanto subcontratante (i.e., se trata os dados pessoais por conta do responsável pelo tratamento dos dados), deverá considerar as implicações de se encontrar sujeito ao RGPD, incluindo quais as obrigações que pode e deve assumir, e as quais poderão ser assumidas pelos seus clientes e terceiros, bem como se os atuais termos e condições necessitam de ser alterados.

Assegure-se que consegue demonstrar que está a cumprir o RGPD.

O RGPD 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 dos dados;
- O tratamento não for ocasional; ou
- 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.

Deverá cooperar com a autoridade de supervisão nacional e disponibilizar os seus registos, se necessário. Com efeito, será aconselhável rever a legislação aplicável à autoridade de supervisão nacional (a CNPD, em Portugal), os respetivos poderes e procedimentos.

Adapte os seus procedimentos por forma a realizar uma avaliação de impacto do tratamento de dados.

Uma avaliação de impacto das operações de tratamento de dados será exigível se os tratamentos forem suscetíveis de implicar um risco elevado para os seus titulares.

Embora sejam ainda escassos os requisitos que permitem definir o conceito de "risco elevado", o tratamento poderá ser de risco elevado se impedir os titulares dos dados de exercerem um direito, utilizarem um serviço ou celebrarem um contrato, ou nos casos em que o tratamento seja sistematicamente efetuado em larga escala.

Poderá ser importante analisar as decisões e orientações publicadas pelas autoridades de supervisão nacional dos países onde recolhe dados de forma a determinar que atividades podem ser consideradas de "risco elevado". As decisões da CNPD encontram-se publicadas em www.cnpd.pt.

A avaliação de impacto sobre a proteção de dados tem por objetivo avaliar a origem, natureza, exatidão e gravidade dos riscos e implementar medidas de segurança para os mitigar, como é o caso da encriptação, e assegurar um nível de segurança apropriado.

Caso não consiga mitigar o risco elevado através de medidas apropriadas face à tecnologia existente e custos de implementação, deverá consultar a autoridade de supervisão nacional antes de proceder a qualquer tratamento de dados pessoais.

3. Tenha em conta os novos direitos dos titulares dos dados.

Assegure-se que consegue cumprir e/ou cumpre o "direito de portabilidade" dos titulares dos dados.

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 corrente 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 responsável pelo tratamento a quem foram fornecidos o possa impedir.

Isto significa que poderá ter de implementar determinadas medidas técnicas, e.g. permitir o "download" direto dos dados pelos titulares ou disponibilizar um interface de programação de aplicações (API), etc..

Os titulares podem querer, eles próprios, armazenar os seus dados ou recorrer a um terceiro para o efeito, concedendo acesso aos responsáveis pelo tratamento.

Assegure-se que consegue cumprir e/ou cumpre o "direito a ser esquecido" dos titulares de dados.

O "direito a ser esquecido" (designado "direito ao apagamento") significa que os titulares dos dados têm direito de 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.

O direito a ser esquecido encontra-se, todavia, sujeito a algumas exceções, e.g., para 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, para fins de investigação científica ou histórica.

Tenha em conta que o RGPD prevê a obrigação de o responsável pelo tratamento de apagar os dados pessoais, a pedido do titular, sem demora justificada.

Isto significa que poderá ter de alterar ou atualizar os seus procedimentos para poder satisfazer os pedidos de apagamento dos titulares dos dados, nomeadamente quanto aos meios utilizados e tempo necessário para proceder à eliminação dos dados.

4. Assegure-se que os seus colaboradores 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 nos seio da sua organização. Poderá ser necessário:

- Criar uma função específica para desempenhar a função de EPD;
- Designar um único EPD para todo o seu negócio; ou
- Designar um EPD para cada estabelecimento ou jurisdição do seu 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 seja obrigatório, poderá ser aconselhável designar um EPD por forma a centralizar as questões de proteção de dados e facilitar o cumprimento do RGPD, o que poderá ser recomendável se os seus colaboradores (e.g. Recursos Humanos, Departamento Comercial) não estiverem conscientes da relevância das regras de proteção de dados.

O RGPD requer a designação de um EPD em três casos específicos:

- Quando o tratamento for efetuado por uma autoridade ou 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. E.g. serviços de telecomunicações, concessão de crédito a clientes, seguradoras; ou
- Quando as atividades principais do responsável ou subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados (dados genéticos, dados biométricos, dados de saúde) ou dados pessoais relacionados com condenações penais e infrações. E.g. tratamento de dados relativos à saúde de pacientes por hospitais.

A designação de um EPD não se encontra ligada à dimensão da empresa, mas sim à sua atividade principal e categorias de dados tratados. Empresas de grande dimensão, que recolham dados para processamento de salários dos seus colaboradores, não estão necessariamente obrigadas a designar um EPD.

5. Adote 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 aplique, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, medidas técnicas e organizativas adequadas destinadas a aplicar com eficácia os princípios da proteção de dados e a incluir garantias necessárias no tratamento, de forma a que este proteja os direitos dos titulares dos dados.

Estas medidas podem incluir:

- Minimização do tratamento de dados;
- Pseudonimização de dados pessoais o mais cedo possível;
- Adoção de medidas 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).

As medidas de “proteção por defeito” devem assegurar que, por defeito, os dados pessoais não são disponibilizados sem intervenção humana a um número indeterminado de pessoas.

As empresas devem determinar, de forma casuística, as medidas adequadas para fazer cumprir estes requisitos.

Um procedimento de certificação aprovado pode ser utilizado como forma de garantir o cumprimento das exigências da proteção “desde a conceção” e da proteção “por defeito”.

É, todavia, de salientar que um procedimento de certificação poderá ainda levar algum tempo a ser adotado e revelar-se uma opção eventualmente morosa e dispendiosa.

6. Reveja e atualize as medidas de segurança do tratamento.

Reveja e atualize as suas medidas de segurança.

O RGPD prevê a aplicação das seguintes medidas técnicas e organizativas:

- Pseudonimização e cifragem dos dados pessoais;
- Capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- Capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico; e
- Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Estas medidas só se aplicam "consoante o que for adequado", o que significa que não são obrigatórias em todos os casos, permitindo à empresa o direito de optar por outras medidas. 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.

Implemente um procedimento de notificação em caso de violação de dados pessoais.

Em caso de violação de dados pessoais, o responsável pelo tratamento de dados:

- Deverá notificar a violação à autoridade de supervisão, sem demora injustificada e, sempre que possível, até 72 horas após seu conhecimento, a menos que seja possível demonstrar que a violação de dados pessoais não é suscetível de resultar num risco para os direitos dos titulares dos dados; e/ou
- Deverá informar o titular dos dados, sem demora injustificada (o RGPD não prevê um prazo específico para o efeito), quando a violação seja suscetível de implicar um elevado risco para os direitos do titular dos dados, em cooperação com a autoridade de supervisão.

Assim, deverá estar preparado para o seguinte: (i) confirmar que todas as medidas de segurança técnicas e organizativas adequadas foram adotadas para prevenir uma violação de dados pessoais, (ii) ser capaz de determinar, de forma imediata, que ocorreu uma violação de dados e (iii) informar, em tempo útil, a autoridade de supervisão e o titular dos dados, se necessário.

7. Reveja o impacto sobre as transferências transfronteiriças de dados.

O RGPD mantém e reforça as atuais regras sobre transferências internacionais de dados, que são permitidas, desde que apresentem garantias adequadas. A par das soluções existentes, como as "cláusulas contratuais-tipo" e o consentimento do titular, prevêem-se ainda novas soluções para justificar as transferências transfronteiriças.

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

O consentimento do titular dos dados mantém-se também como uma das opções possíveis para justificar a transferência internacional de dados. Em determinados casos poderá, no entanto, revelar-se difícil de obter, uma vez que o consentimento tem de ser explícito e dado através de um ato positivo inequívoco, específico, livre e informado.

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 não serem aplicáveis entre entidades subcontratantes, as regras vinculativas estarão disponíveis tanto para responsáveis pelo tratamento como para subcontratantes.

As jurisdições "permitidas", ou seja, os países para os quais é permitido transferir dados pessoais na medida em que possuem legislação sobre proteção de dados adequada, por ser "essencialmente equivalente" ao RGPD, é outra das soluções. A constatação de adequação será revista a cada 4 anos.

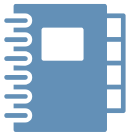
O "Escudo de Proteção da Privacidade" de dados UE-EUA, que vem substituir o anterior acordo "Safe Harbor", invalidado no caso "Schrems" em 2015 pelo Tribunal de Justiça da UE, é outra opção, que tem por objetivo agilizar as transferências de dados da UE para os EUA, assegurando um nível de proteção adequado no tratamento dos dados de cidadãos europeus por empresas sedeadas nos EUA.

Códigos de conduta acompanhados de compromissos vinculativos dos responsáveis pelo tratamento ou dos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, ou a criação de procedimentos de certificação constituem novas soluções para as transferências de dados para países terceiros.

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 notificação à autoridade de supervisão e prestação de informação ao titular dos dados.

A SUA LISTA DE TAREFAS

- A ideia-chave é "mapear" todos os dados utilizados pela sua empresa. Solicite a cada um dos departamentos para especificar numa tabela as diferentes categorias de dados que usam, para que finalidades, por quanto tempo, etc..
- Organize uma auditoria aos dados com os departamentos de RH, comercial, IT e jurídico para perceber que dados são tratados, como são geridos e que medidas de segurança estão a ser adotadas.



- Reveja a sua política de privacidade ("como usamos a sua informação") e o consentimento dos titulares dos dados.
- Reveja os contratos com os subcontratantes. Se é um subcontratante, avalie que obrigações poderá assumir e quais poderão ser assumidas pelos seus clientes e terceiros.
- Reveja procedimentos para aferir se os titulares dos dados podem exercer os seus direitos (e.g. direito "à portabilidade dos dados" e "a ser esquecido").

- Considere designar um único Encarregado de Proteção de Dados ou proceder a designações individuais para cada estabelecimento e/ou jurisdição do seu grupo.
- Assegure formação adequada aos seus colaboradores em matéria de procedimentos, políticas internas, etc.. Envolva o seu departamento jurídico nestas ações.

- Reveja e atualize as suas políticas internas e medidas técnicas com a ajuda da sua equipa de IT por forma a cumprir os requisitos de proteção "desde a conceção" e "por defeito".
- Reavalie as suas medidas de segurança.
- Implemente um sistema de notificação em caso de violação de dados e teste periodicamente a eficácia das suas medidas técnicas e organizativas.

- Verifique qual será o impacto do RGPD nas suas atuais transferências internacionais de dados e se estas continuam a ser justificadas.
- Considere adotar uma "solução-chave" com o seu departamento jurídico para obter uma justificação abrangente para as suas transferências internacionais de dados, e.g. cláusulas contratuais-tipo, regras vinculativas aplicáveis às empresas, códigos de conduta ou certificação.

QUEM SOMOS

A nossa prática em Proteção de Dados

QUEM SOMOS

A Macedo Vitorino & Associados foi fundada em 1996, centrando a sua atividade na assessoria a clientes nacionais e estrangeiros em sectores específicos de atividade, de que destacamos o sector financeiro, as telecomunicações, a energia e as infraestruturas.

Desde a nossa constituição, temos estado envolvidos em várias operações de alto nível em todas as áreas de prática da sociedade, incluindo bancário e financeiro, mercado de capitais, societário e M&A, reestruturações empresariais, etc..

Somos mencionados pela publicação "The European Legal 500" na maioria das suas áreas de prática, incluindo "Banking and Finance", "Capital Markets", "Project Finance", "Tax", "Real Estate", "Telecoms" e "Litigation".

Somos ainda mencionados pela "IFLR 1000" em "Project Finance", "Corporate Finance" e "Mergers and Acquisitions" e pela Chambers and Partners em "Banking and Finance", "Corpoate and M&A", "TMT", "Dispute Resolution", "Restructuring and Insolvency".

Assessoramos os nossos clientes em todas as questões relativas a proteção de dados, incluindo:

- Preparar e apresentar notificações e pedidos de autorização junto da Comissão Nacional de Proteção de Dados;
- Preparar programas de «compliance», elaborar e rever políticas de privacidade e notificações para transferências transfronteiriças de dados;
- Elaborar e rever contratos e cláusulas específicas relativas a proteção de dados, incluindo contratos de software, subcontratação e licenciamento;
- Prestar assessoria a operações de transferências internacionais de dados;
- Rever soluções tecnológicas, incluindo sistemas de «cloud» e de geolocalização;
- Assegurar o cumprimento legal de normas de proteção de dados em sectores específicos, como bancário e financeiro, saúde, telecomunicações e media, tecnologia de informação e comércio eletrónico.

Se quiser saber mais sobre a Macedo Vitorino & Associados por favor visite o nosso website www.macedovitorino.com ou contacte-nos para mva@macedovitorino.com.

Cláudia Fernandes Martins
cmartins@macedovitorino.com

Rua do Alecrim 26E | 1200-018 Lisboa | Portugal
Tel.: (351)21 324 19 00 | Fax: (351)21 324 19 29
www.macedovitorino.com