Evite multas: 10 dicas de sobrevivência ao RGPD

RGPD

Evite multas: 10 dicas de sobrevivência ao RGPD

Cláudia Fernandes Martins

O Regulamento Geral de Proteção de Dados ("RGPD"), que passou a ser aplicável a partir de 25 de maio de 2018, é um dos temas incluído na agenda das organizações no último ano, embora, a sua maioria (em particular PME e o sector público), ainda se encontrem atrasadas na sua implementação.

O RGPD vem mudar o "paradigma" existente, ao estabelecer um "princípio de responsabilidade", em que as organizações passam a ter um papel proativo na interpretação e aplicação das regras de proteção de dados pessoais, sob pena de, em caso de incumprimento, ficarem sujeitas a pesadas coimas, que podem atingir os 20 milhões de euros ou 4% do volume de negócios anual do grupo, consoante o mais elevado.

Se a sua organização pertence àquela maioria, que ainda está atrasada na implementação do RGPD, eis as principais "dicas" que precisa de saber para começar a pôr "mãos à obra". Não terá de ser necessariamente uma tarefa complexa, mas exigirá alguma paciência, um profundo conhecimento da organização, acompanhado por uma partilha de tarefas e de repartição de responsabilidades, para já não falar de uma mudança de práticas instituídas e de mentalidades.

Assim:

1. Identifique que dados são recolhidos e utilizados pela sua organização

Comece por "mapear" os dados recolhidos e utilizados pela sua organização e depois agrupá-los em conjuntos identificáveis, funcionais e com riscos similares ao nível da sua proteção e conservação, tendo em conta: (i) as categorias de dados, por exemplo, dados de identificação, dados de faturação, dados de saúde, etc.; (ii) a finalidade de tratamento, por exemplo, gestão de recursos humanos, marketing, etc.; (iii) o prazo de conservação; (iv) o âmbito geográfico do tratamento; (v) quem tem acesso aos dados e com quem são partilhados; (vi) as medidas de segurança em curso.

2. Reveja os seus procedimentos, políticas, contratos e outra documentação relevante

Reveja a sua política de privacidade, ou seja, o documento pelo qual informa os titulares dos dados de como são recolhidos e utilizados os seus dados pela sua organização.

Se o tratamento está a ser realizado porque obteve um prévio consentimento do titular dos dados, deverá confirmar se esse consentimento se mantém válido e se será capaz de o demonstrar. 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 também designados por "categorias especiais de dados" (por exemplo, dados relativos à saúde, dados genéticos, biométricos, convicções políticas, religião, orientação sexual) ou transferência de dados para fora da UE, o consentimento tem de ser explícito. O silêncio, opções pré-validadas ou a omissão do titular dos dados não constituem consentimento.

Tenha ainda em atenção que o consentimento é apenas um dos fundamentos que permitem justificar o tratamento de dados (ou de determinados dados), mas podem existir outros fundamentos, por exemplo, 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, ou se for necessário para efeito do interesse legítimo prosseguido pela organização. Se assim for, não precisa de obter o prévio consentimento. Sabia, por exemplo, que o RGPD permite que o tratamento realizado para fins de marketing direto poderá, em determinados casos, ser justificado pelo interesse legítimo da organização, e desde que seja assegurado o direito de a qualquer momento o titular dos dados se opor a receber comunicações para essa finalidade.

Se a sua organização recorre a entidades subcontratadas para, por sua conta e segundo as suas instruções, tratarem dados pessoais (por exemplo, recurso a uma empresa externa de contabilidade, de medicina do trabalho, de informática, de arquivo, de segurança privada), deverá atualizar o seu acordo com essas entidades. Esse acordo tem de ser escrito e incorporar a nova terminologia e obrigações impostas pelo RGPD.

3. Tenha em conta os direitos dos titulares dos dados e adote procedimentos que permitam o exercício desses direitos

Por forma a promover uma relação de lealdade e transparência entre a organização e os titulares dos dados, os denominados direitos "ARCO" (acesso, retificação, cancelamento e oposição) dos titulares dos dados são reforçados pelo RGPD, em particular pelo direito à informação, "direito à portabilidade" e "direito a ser esquecido".

O RGPD vem impor que a organização informe/dê acesso, a pedido dos titulares dos dados, às atividades de tratamento dos seus dados e isto de forma gratuita e no prazo de um mês, bem como que o titular dos dados receba os dados pessoais, que tenha fornecido, num formato estruturado, de uso corrente e de leitura automática, e possa solicitar que os seus dados sejam transmitidos, de forma gratuita, a outra organização. Pense-se, por exemplo, no caso de mudança de operador de comunicações, de instituição bancária.

A sua organização deverá ainda assegurar-se que consegue cumprir e/ou cumpre com o "direito a ser esquecido", o direito de a pedido do titular proceder ao apagamento dos seus dados pessoais, sem demora injustificada, e abster-se de qualquer disseminação futura dos dados.

4. 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 a organização 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 (por exemplo, pseudonimização, encriptação dos dados).

Já a "proteção por defeito" requer que a sua organização 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 organizações 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".

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

O RGPD impõe que as organizações criem e mantenham um registo das atividades de tratamento se:

– Tiverem mais de 250 trabalhadores;
– O tratamento de dados for suscetível de implicar um risco para os direitos do titular dos dados e 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 controlo e disponibilizar os seus registos, se necessário.

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

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.

A 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, nomeadamente, nos casos de definição de perfis, tratamento de dados sensíveis em grande escala ou recurso a sistemas de videovigilância em grande escala.

Caso não consiga mitigar o risco elevado através de medidas apropriadas face à tecnologia existente e custos de implementação, deverá consultar a autoridade de controlo (a Comissão Nacional de Proteção de dados, em Portugal) antes de proceder ao tratamento de dados pessoais.

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

A designação de um DPO não se encontra ligada à dimensão da organização, mas sim à sua atividade principal e categorias de dados tratados. O RGPD impõe a designação de um DPO, que poderá ser um colaborador ou uma entidade ou pessoa externa à sua organização, em três casos específicos:

– Quando o tratamento for efetuado por uma autoridade ou organismo público (exceto tribunais);
– Quando as atividades principais da organização ou do subcontratado a recorra consistam em operações de tratamento que exijam um controlo sistemático e regular dos titulares dos dados em grande escala. Por exemplo, serviços de telecomunicações, concessão de crédito a clientes, seguradoras; ou
– Quando as atividades principais da organização ou do subcontratado a que recorra consistam em operações de tratamento em grande escala de dados sensíveis (dados genéticos, dados biométricos, dados de saúde) ou dados pessoais relacionados com condenações penais e infrações. Por exemplo, tratamento de dados relativos à saúde de pacientes por hospitais.

Mesmo quando não seja obrigatório, poderá ser aconselhável designar um DPO por forma a centralizar as questões de proteção de dados e facilitar o cumprimento do RGPD pela sua organização.

8. Reveja e atualize as medidas de segurança do tratamento e implemente um procedimento de notificação em caso de violação de dados pessoais

A sua organização deverá estar preparada para: (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 controlo e o titular dos dados, se necessário.

Em caso de violação de dados pessoais, deverá adotar procedimentos por forma a notificar a violação à autoridade de controlo, 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. Também 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, e em cooperação com a autoridade de controlo.

9. Reveja o impacto sobre as transferências internacionais de dados

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, por exemplo, regras vinculativas aplicáveis a entidades de um grupo empresarial, que realizem entre si transferências de dados; códigos de conduta acompanhados de compromissos vinculativos das organizações no país terceiro no sentido de aplicarem as garantias adequadas, ou a criação de procedimentos de certificação.

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.

10. Assegure-se que os seus colaboradores estão conscientes das implicações do RGPD e têm formação sobre as novas regras

Esta medida aparece, em último lugar, mas também poderia aparecer em primeiro ou, na verdade, em qualquer uma das posições anteriores. Trata-se de uma medida transversal e necessária à implementação do RGPD ao longo do tempo e essencial para a consciencialização sobre o tema e uma progressiva mudança de mentalidades no seio das organizações.

Cláudia Martins, advogada da Macedo Vitorino & Associados