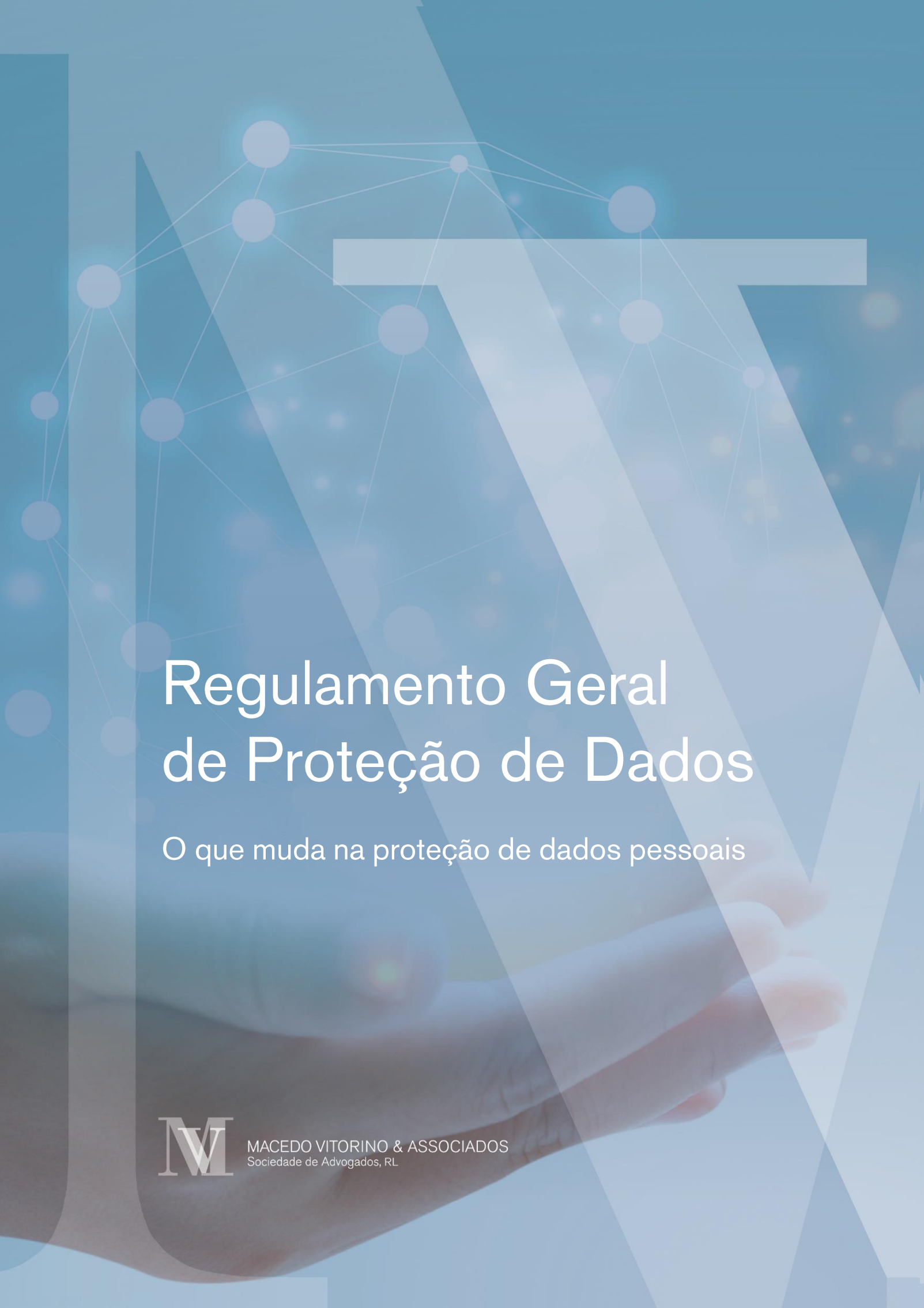

Regulamento Geral de Proteção de Dados

O que muda na proteção de dados pessoais

MACEDO VITORINO & ASSOCIADOS
Sociedade de Advogados, RL

Sobre nós

A Macedo Vitorino & Associados é um dos principais escritórios de advocacia portugueses. Aconselhamos clientes nacionais e estrangeiros num amplo leque de setores de atividade, nomeadamente no setor financeiro, distribuição, indústria e projetos.

A nossa prática é multifacetada. Assessoramos algumas das maiores empresas nacionais e internacionais em diversos setores de atividade comercial e industrial, assumindo especial relevância, a banca, a indústria, as telecomunicações, capital de risco e a tecnologia.

A Macedo Vitorino & Associados tem uma equipa sólida e experiente que presta assessoria a clientes nacionais e internacionais em todas as questões relacionadas com a proteção de dados pessoais, nomeadamente:

- Preparação e apresentação de notificações e pedidos de autorização junto da Comissão Nacional da Proteção de Dados
- Elaboração de programas de «compliance», políticas de privacidade, contratos e cláusulas específicas relativas a proteção de dados, incluindo contratos de software, subcontratação e licenciamento
- Revisão de questões de segurança e soluções tecnológicas, incluindo sistemas de «cloud» e de geolocalização
- Prestação de assessoria em operações de transferências internacionais de dados
- Assegurar o cumprimento legal de normas de proteção de dados em setores específicos, como bancário e financeiro, saúde, telecomunicações e media, tecnologia de informação e comércio eletrónico

Somos citados na maioria das áreas de trabalho analisadas pelo diretório internacional, Legal 500, nomeadamente em «Banking and Finance», «Capital Markets», «Public Law», «Corporate», «Tax», «Telecoms» e «Dispute Resolution».

A atuação da Macedo Vitorino & Associados é ainda destacada pela IFLR1000 em «Project Finance», «Corporate Finance» e «M&A» e pela Chambers and Partners em «Banking & Finance», «Corporate and M&A», «Tax» e «TMT».

Se quiser saber mais sobre a Macedo Vitorino & Associados visite o nosso website **www.macedovitorino.com**

Introdução

A partir de 25 de maio de 2018, data de aplicação do Regulamento Geral de Proteção de Dados (RGPD), todos os Estados-Membros da União Europeia (UE) passam a estar sujeitos a regras comuns em matéria de proteção de dados pessoais.

Organizações sedeadas fora da UE também podem estar sujeitas ao RGPD quando as suas atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a titulares de dados da UE ou com o controlo do comportamento de titulares de dados, quando este tenha lugar na UE.

Ao contrário da Diretiva 95/46/CE transposta pela Lei n.º 67/98, de 26 de outubro, que aprovou a Lei de Proteção de Dados Pessoais (LPDP), o RGPD aplica-se sem necessidade de ser aprovada legislação nacional e revogará a LPDP. Isto não significa, porém, que, em determinadas matérias (ex. tratamento de dados sensíveis ou de dados de trabalhadores no contexto laboral), não possa vir a ser aprovada legislação nacional específica, que se aplicará em conjunto com o RGPD.

Se compararmos o RGPD com a LPDP parecem não existir alterações significativas ao nível dos princípios de proteção dos dados: os conceitos de dados pessoais e de tratamento, os princípios fundamentais a que devem obedecer os tratamentos de dados e os fundamentos de licitude permanecem intocáveis. As alterações, essas sim significativas, verificam-se ao nível das regras do jogo e da operacionalização destes princípios.

De entre essas alterações é de salientar a mudança do modelo de regulação: o RGPD introduz um modelo de autorregulação, em contraste com o modelo de hétero-regulação da LPDP, o que terá um impacto relevante no dia-a-dia das organizações.

As organizações passam a ser responsáveis pela interpretação e operacionalização das regras de proteção de dados, bem como por assegurar, de forma contínua, e demonstrar o cumprimento do RGPD, ficando sujeitas a fiscalização e supervisão da autoridade de controlo do país do seu estabelecimento principal ou único (sistema de «balcão único»).

As organizações devem, por isso, começar por compreender qual o seu perfil de risco e, a partir deste exercício, ponderar o que devem fazer para atuar em conformidade com o RGPD e demonstrar essa conformidade, sob pena de risco de coimas, que aumentam exponencialmente e que poderão ir até 4% do volume de negócios anual, a nível mundial, ou até 20 milhões de euros, consoante o que for superior.

O consentimento não é o único fundamento

As organizações que realizem tratamentos de dados pessoais devem estar cientes de que essas operações apenas serão válidas se forem justificadas por um dos fundamentos legítimos previstos no RGPD, entre os quais o consentimento.

O consentimento tem de ser dado mediante um acto positivo e claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular consente o tratamento dos seus dados pessoais.

O consentimento pode ser dado por declaração escrita, inclusive em formato eletrónico, por declaração oral ou validando uma opção ao visitar um sítio de Internet. Não valem como consentimento o silêncio, opções pré-validadas ou a omissão. O consentimento tácito não é válido.

A declaração de consentimento deve incluir a identidade do responsável pelo tratamento e as finalidades de tratamento, bem como o consentimento deve abranger todas as atividades de tratamento realizadas com a mesma finalidade e nos casos em que sirva fins múltiplos tem de ser obtido um consentimento para todos esses fins.

O responsável pelo tratamento deve poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados.

O consentimento prévio do titular dos dados, cujos requisitos passam a ser mais exigentes, constitui um dos fundamentos, mas não é o único. Nem sempre será possível recorrer ao consentimento, nomeadamente, quando exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo tratamento, por exemplo, quando o responsável é uma autoridade pública, ou nos casos em que o titular dos dados não disponha de uma escolha verdadeira ou livre, como poderá acontecer no âmbito de uma relação laboral.

Assim e sem necessidade de recorrer ao consentimento, o tratamento de dados será igualmente válido se for necessário para a execução de um contrato no qual o titular dos dados seja parte, o cumprimento de uma obrigação jurídica do responsável pelo tratamento, a defesa de interesses vitais do titular dos dados ou de outra pessoa singular, o exercício de funções de interesse público ou de autoridade pública ou a prossecução de interesses legítimos do responsável ou de terceiros.

Reforço dos direitos dos titulares dos dados

O RGPD continua a garantir, a todo o tempo, aos titulares dos dados os direitos de acesso, atualização, retificação e cancelamento dos dados, bem como, se for o caso, de oposição ao tratamento – os denominados direitos «ARCO». Os titulares dos dados poderão ainda opor-se ao tratamento dos dados para fins de marketing.

O RGPD reforça ainda o direito à informação dos titulares dos dados e prevê dois novos direitos: o direito à portabilidade dos dados e o direito a ser esquecido.

Quanto à informação a prestar aos titulares dos dados, o RGPD impõe a prestação de informação adicional, nomeadamente, quanto ao fundamento legal para o tratamento, prazo de conservação dos dados, transferências internacionais de dados e possibilidade de queixa junto da autoridade de controlo.

A informação deve ser prestada numa linguagem clara e simples e de fácil acesso, no prazo de um mês a contar da data de receção do pedido do titular dos dados (com possibilidade de prorrogação até dois meses, em alguns casos) e a título gratuito. Deve ser dado particular cuidado quando as informações sejam dirigidas a crianças.

O direito à portabilidade aplica-se aos dados pessoais tratados através de meios automatizados (ficam excluídos os dados tratados em suporte de papel) e consiste no direito do titular a receber os seus dados pessoais do responsável pelo tratamento, para que os possa reutilizar na sua esfera privada, bem como no direito de exigir que o responsável pelo tratamento comunique os seus dados pessoais a um outro responsável. O direito à portabilidade apenas poderá ser exercido quanto aos dados pessoais que tenham sido recolhidos com o consentimento do titular, ou cujo tratamento seja necessário para o cumprimento de um contrato.

Por exemplo, nos casos em que os clientes pretendam mudar de operador de Internet, poderão mover os seus dados, incluindo os gerados com a sua atividade (ex. *playlists*, históricos de pesquisa, dados de trânsito ou localização) para um novo operador. Para permitir a reutilização dos dados, estes terão de ser entregues pelo responsável, num formato estruturado, de uso corrente, de leitura automática e interoperável.

O titular tem ainda direito de obter o apagamento dos seus dados pessoais, sem demora injustificada – direito a ser esquecido –, salvo, entre outros, para cumprimento de uma obrigação legal, motivos de interesse público no domínio da saúde pública, arquivo de interesse público, fins de investigação científica, histórica ou estatísticos.

Partilha de responsabilidades

As organizações devem adotar medidas técnicas e organizativas adequadas e eficazes, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como o risco para os titulares dos dados. Em particular, devem aplicar medidas que respeitem os princípios da proteção de dados desde a conceção e por defeito e, entre outras, a minimização do tratamento, a pseudonimização e a possibilidade de o titular controlar o tratamento.

Uma avaliação de impacto das operações de tratamento de dados será exigível se essas operações forem suscetíveis de implicar um risco elevado para os titulares, por exemplo, quando esteja em causa a definição de perfis, por meios automatizados, para a celebração de um contrato, ou tratamentos em grande escala de dados de saúde, biométricos, genéticos, ou de dados relacionados com condenações penais e infrações, ou de controlo sistemático de zonas acessíveis ao público em grande escala.

Caso não seja possível mitigar o risco elevado através de medidas apropriadas face à tecnologia existente e custos de implementação, a organização deve consultar a autoridade de controlo antes de proceder ao tratamento dos dados.

Em caso de violação de dados, a organização é obrigada a comunicar essa violação, no prazo máximo de 72 horas, a contar do seu conhecimento, à autoridade de controlo e, quando for provável que dessa violação resulte um elevado risco para o titular dos dados, a dar-lhe conhecimento, sem demora injustificada.

Quando uma operação de tratamento de dados seja efetuada com recurso a subcontratação, ou seja, por um terceiro, por conta do responsável pelo tratamento, o RGPD prevê obrigações diretas para o subcontratado.

A subcontratação está sujeita a acordo escrito. Os subcontratados têm de oferecer garantias suficientes, em termos de conhecimentos especializados, fiabilidade e recursos, quanto à execução de medidas técnicas e organizativas, em particular quanto à segurança do tratamento, e não podem eles próprios subcontratar terceiros sem que o responsável pelo tratamento tenha dado autorização prévia e por escrito.

Os subcontratados devem documentar de forma detalhada todas as atividades de tratamento de dados, tanto as que resultam diretamente da obrigação de manter um registo como as relativas a outros procedimentos internos.

O «Encarregado da Proteção de Dados»

As organizações, que tratem dados pessoais, passam a ser obrigadas a designar um Encarregado da Proteção de Dados (*Data Protection Officer* - «DPO»), quando:

- Sejam um organismo ou autoridade pública (exceto tribunais);
- As suas atividades principais consistam em operações de tratamento que exijam o controlo regular e sistemático de titulares dos dados em grande escala. Por exemplo, serviços de telecomunicações, concessão de crédito a clientes, seguradoras; ou
- As suas atividades principais consistam em operações de tratamento em grande escala de categorias especiais de dados pessoais (dados genéticos, biométricos, de saúde) e dados pessoais relacionados com condenações penais e infrações. Por exemplo, tratamento de dados relativos à saúde de pacientes por hospitais.

As atividades principais referem-se às atividades primárias e não ao tratamento de dados como uma atividade auxiliar da organização, como pode ser, por exemplo, o processamento de salários.

As funções do Encarregado da Proteção de Dados são, entre outras, as seguintes:

- Dever de informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados sobre as respetivas obrigações legais;
- Dever de controlar a conformidade com o RGPD, incluindo com outras disposições de proteção de dados e com as políticas do responsável ou do subcontratante, incluindo repartição de responsabilidades, sensibilização e formação do pessoal;
- Dever de prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e de controlar a sua realização; e
- Dever de cooperar com a autoridade de controlo, sendo o ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento.

O nível necessário de conhecimentos especializados do Encarregado da Proteção de Dados deve ser determinado, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados.

O Encarregado da Proteção de Dados poderá ser um trabalhador ou terceiro contratado externamente pela organização, à qual compete assegurar que do exercício das suas funções não resulta um conflito de interesses e que são desempenhadas com independência face à própria organização e com reporte direto à administração.

Solução-chave para fluxos transfronteiriços

O RGPD reforça as regras sobre transferências de dados para países fora da UE. São permitidas, desde que sejam dadas garantias adequadas pelo país para onde os dados são transferidos.

O RGPD prevê soluções que podem ser utilizadas para estabelecer garantias adequadas e sem necessidade de autorização prévia da autoridade de controlo.

Dependendo do caso, podem ser adotadas, entre outras, as seguintes soluções:

- Adesão a cláusulas contratuais tipo aprovadas pela Comissão Europeia, que se aplicam a transferências de dados entre responsáveis pelo tratamento ou entre um responsável pelo tratamento e um subcontratante, mas já não a transferências de dados entre subcontratantes. A circunstância de as cláusulas não poderem ser alteradas também nem sempre funcionará para todos os casos;
- Obtenção de consentimento prévio do titular dos dados, o qual se mantém, ainda que, em determinados casos, possa revelar-se difícil de cumprir com os exigentes requisitos do consentimento impostos pelo RGPD, uma vez que tem de ser explícito e traduzir-se num ato positivo inequívoco, específico, livre e informado;
- Adoção de regras vinculativas aplicáveis às empresas, ao abrigo das quais as entidades de um grupo empresarial podem vincular-se a realizar entre si transferências de dados;
- Aplicação das jurisdições «permitidas», como é o caso das transferências de dados para a Suíça, Canadá, Andorra, Argentina, Nova Zelândia, Israel, de acordo com decisões aprovadas pela Comissão Europeia, que revê a adequação a cada quatro anos;
- Adesão ao «Escudo de Proteção da Privacidade» (*Privacy Shield*) para transferências de dados da UE para os Estados Unidos da América, aprovado pela Decisão da Comissão Europeia de 12 de julho de 2016, e que veio substituir o acordo de «Porto Seguro» (*Safe Harbor*), considerado inválido pelo acórdão «Schrems» em 2015 pelo Tribunal de Justiça da UE;
- Códigos de conduta acompanhados de compromissos vinculativos das entidades no país terceiro ou processos de certificação aprovados.

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

Multas pesadas

O RGPD impõe severas coimas, que podem ir até 20 milhões de euros ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o que for mais elevado, nos casos, entre outros, de violação de:

- Princípios básicos do tratamento (licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade), incluindo as condições de consentimento;
- Direitos dos titulares dos dados (direitos «ARCO», direito de portabilidade e direito a ser esquecido);
- Regras aplicáveis às transferências internacionais de dados pessoais; e
- Obrigações relativas a situações específicas de tratamento nos termos do direito de um Estado-Membro (por exemplo, tratamento no contexto laboral).

Dependendo da infração, as coimas podem ir até aos10 milhões de euros ou, no caso de uma empresa, até 2% do seu volume de negócios anual, consoante o que for mais elevado, nos casos, entre outros, de:

- Violação das obrigações quanto à proteção de dados desde a conceção e por defeito, bem como das obrigações aplicáveis à relação entre o responsável pelo tratamento e a entidade subcontratada, por exemplo, falta de acordo escrito com a entidade subcontratada, recurso do subcontratado a subcontratação sem acordo prévio por escrito do responsável pelo tratamento;
- Falta de registo das atividades de tratamento de dados, realização de avaliação de impacto ou de designação de um Encarregado da Proteção de Dados, nos casos em que seja obrigatório;
- Violação das regras de segurança do tratamento e falta de notificação da violação de dados à autoridade de controlo e de comunicação ao titular dos dados, nos casos em que seja exigível.

As pessoas que tenham sofrido prejuízos em consequência da violação do RGPD têm o direito a pedir indemnização ao responsável pelo tratamento ou à entidade subcontratada, a qual será solidariamente responsável se não tiver cumprido as obrigações que lhe sejam especificamente dirigidas ou se não tiver seguido as instruções do responsável pelo tratamento.

Glossário

Autoridade de controlo: autoridade pública independente que é responsável pela fiscalização da aplicação do RGPD em cada Estado-Membro da UE. No caso português, a Comissão Nacional de Proteção de Dados (CNDP).

Dados pessoais: informação relativa a uma pessoa singular (mas já não a uma pessoa coletiva) identificada ou identificável, como, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrónica, um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social da pessoa singular. Os dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, os dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual são categorias especiais de dados.

Finalidades de tratamento: fins visados com as operações de tratamento de dados, como seja, a título de exemplo, a gestão de recursos humanos, gestão de clientes, marketing, faturação, gravação de chamadas para monitorização da qualidade de um serviço.

Meios de tratamento: os dados pessoais podem ser tratados por meios automatizados (ou seja, com recurso a meios tecnológicos) ou não automatizados (ou seja, através de tratamento manual). Nos casos de tratamento manual, o RGPD só se aplicará se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros.

Subcontratante: uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento, ou seja, de acordo com as instruções deste.

Responsável pelo tratamento: a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

Titular dos dados: pessoa singular (mas já não uma pessoa coletiva) identificada ou identificável a quem os dados pessoais dizem respeito. É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a determinados dados.

Tratamento de dados: uma operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

© 2018 Macedo Vitorino & Associados

“Excellent. Very good lawyers with the ability to provide tailor made solutions, and a different approach to problem solving.”

IFLR1000

“Very efficient, detailed and thorough when presenting solutions and addressing the issues; we were impressed.”

Chambers and Partners

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