O NOVO REGULAMENTO DE PROTEÇÃO DE DADOS

OPORTUNIDADES E DESAFIOS

MACEDO VITORINO & ASSOCIADOS
Sociedade de Advogados, RL

Aspetos gerais do Regulamento

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril, publicado 4 de maio de 2016, vai trazer importantes alterações às regras de proteção de dados pessoais.

As atuais leis de proteção de dados serão revogadas quando o Regulamento entrar em vigor a 25 de maio de 2018. Até lá, as empresas terão de se adaptar e preparar para novas oportunidades:

- O Regulamento é bastante severo, prevê coimas muito pesadas, podendo atingir o montante de € 20.000.000 ou 4% do volume de negócios anual da empresa.
- O Regulamento facilitará as operações intracomunitárias e reduzirá bastante alguns custos administrativos.
- As empresas com atividades dispersas pelos diversos Estados-Membros terão de contactar apenas com a Autoridade de Controlo onde tenham o estabelecimento principal.
- As autoridades de controlo estão mais articuladas, reduzindo os custos burocráticos suportados pelas empresas.
- A nomeação de um encarregado para a proteção de dados (*Data Protection Officer*) será obrigatória para muitas empresas, devendo este observar o cumprimento do Regulamento e lidar diretamente com os titulares dos dados.
- A transferência de dados para países terceiros é muito facilitada, são possibilitadas transferências através de códigos de conduta, certificações e regras vinculativas aplicáveis às empresas.
- A subcontratação de outras empresas para o tratamento dos dados será mais fácil.
- O direito ao esquecimento e à portabilidade dos dados são reconhecidos.
- As empresas terão de comunicar de forma concisa, transparente, inteligível e de fácil acesso com os titulares dos dados, não podendo o tempo de resposta exceder 1 mês.

Direitos e âmbito de aplicação

Direitos dos Titulares

Os cidadãos europeus veem reforçados os seus direitos. A definição de dados pessoais é alargada e atualizada face aos desafios contemporâneos. Além dos dados previstos anteriormente, adicionam-se os “dados de localização” e os “identificadores por via eletrónica”.

Novas definições

Constam, ainda, as definições de "dados biométricos e "dados relativos à saúde", "dados genéticos“, "definição de perfis", "pseudonimização“, “tratamento transfronteiriço” e “violação de dados pessoais”.

O consentimento

O conceito de “consentimento” para além dos critérios anteriores exige, ainda que seja através de declaração ou ato positivo inequívoco, ou seja, por escrito.

Restrições dos Estados-Membros

Os Estados-Membros podem legislar de modo a restringir o tratamento de determinadas categorias de dados, mesmo havendo consentimento do titular.

Crianças e jovens

O Regulamento fixa em 16 anos a idade legal para se poder consentir no tratamento de dados pessoais, nos restantes casos é necessário o consentimento dos titulares das responsabilidades parentais da criança. Os Estados-Membros têm liberdade para reduzir para até 13 anos a idade legal do consentimento.

Âmbito de aplicação

O âmbito de aplicação do Regulamento é bastante alargado. Aos responsáveis pelo tratamento de dados pessoais ou às entidades subcontratadas residentes no território da EU, é aplicado o Regulamento independentemente do tratamento se ocorrer ou não dentro do espaço da União Europeia (“UE”).

O Regulamento prevê o desencadeamento de um efeito extraterritorial (isto é, aplicação a entidades responsáveis pelo tratamento não localizadas na UE) sempre que estejam relacionados com atividades de:

- Oferta de bens ou serviços a titulares de dados na União, independentemente da onerosidade do bem; ou
- Controlo de comportamentos dentro do Espaço da União.

Coesão entre as Autoridades

O Comité Europeu

O Regulamento prevê, em substituição do atual Grupo de trabalho para a Proteção de Dados, a criação do Comité Europeu para a Proteção de Dados, um órgão independente, composto pelos representantes das 28 autoridades nacionais de Controlo e da Autoridade Europeia para a Proteção de Dados.

O Comité assume um papel determinante na concretização do procedimento de controlo da coerência, visto que todas as jurisdições europeias, a partir de 2018, em matéria de proteção de dados regem-se pelo presente Regulamento.

A forma de atuação do Comité

O Comité poderá emitir, para além das diretrizes e recomendações, decisões vinculativas em caso de litígio entre diferentes autoridades de controlo. As decisões cabem, em regra, a uma maioria simples dos representantes deste órgão.

As atribuições do Comité

Este órgão emitirá pareceres prévios sobre algumas medidas que as autoridades locais pretendam adotar.

O Comité assumirá especial relevância na garantia da coesão e da cooperação entre as autoridades locais e a autoridade de controlo principal, sendo ainda um órgão de aconselhamento da Comissão na aplicação do presente Regulamento dentro da União Europeia e nas relações com países terceiros.

Derrogação do Procedimento de controlo da coerência

As autoridades locais podem adotar medidas provisórias (prazo não superior a três meses) em derrogação do Procedimento de controlo da coerência, sempre que seja urgente a defesa dos direitos e liberdades dos titulares dos dados.

Subcontratação

Subcontratantes

Os subcontratantes estão agora diretamente sujeitos à regulação das autoridades de controlo. Os responsáveis pelo tratamento devem apenas escolher subcontratantes que possuam uma estrutura apta a garantir as medidas de segurança regulamentadas.

Restrições na subcontratação

O Regulamento prevê obrigações específicas do subcontratante:

- processa mediante instruções dos responsáveis;
- utilização de medidas técnicas e organizativas adequadas para dar cumprimento ao Regulamento;
- exclui ou retorna os dados ao responsável quando completa o tratamento; e
- disponibiliza todas as informações ao responsável (mantendo em registos).

Autorização

Apenas é permitida a subcontratação autorizada pelo titular dos dados. O responsável pelo tratamento tem de autorizar a subcontratação pelo subcontratante.

Tratamento conjunto

O Regulamento possibilita o tratamento conjunto por dois os mais responsáveis, sendo a responsabilidade repartida. Estes deverão previamente acordar as responsabilidades e os deveres de cumprimento das disposições do Regulamento.

A essência do acordo deve ser disponibilizada aos titulares dos dados. O acordo pode designar um ponto de contacto, entre os responsáveis, para com os titulares do dados.

Independentemente da repartição de responsabilidades, os titulares dos dados podem exercer os seus direitos perante qualquer um dos responsáveis.

Responsabilidade pela violação de dados pessoais

O responsável pelo tratamento deve articular-se bem com o subcontratante, e comunicar no prazo máximo de 72 horas qualquer violação de dados pessoais dos titulares à Autoridade de Controlo.

Responsabilidade do subcontratante

O subcontratante é apenas responsável se não tiver cumprido as obrigações que lhe são dirigidas ou se não tiver seguido as instruções do responsável pelo tratamento.

Data Protection Officer

Encarregado da proteção de dados

O Regulamento prevê a obrigação de ser designado um encarregado da proteção de dados nas seguintes situações:

- o tratamento é efetuado por uma autoridade ou um organismo público;
- quando as atividades principais da organização/empresa (responsável pelo tratamento ou através de subcontratante) exijam um controlo regular e sistemático dos titulares dos dados em grande escala. A organização/empresa terá de considerar a natureza, dimensão e finalidade do tratamento, de modo a verificar a necessidade de nomear um encarregado;
- quando a organização/empresa processa em grande escala "categorias especiais de dados pessoais" (anteriormente, designados dados sensíveis) ou dados relacionados com "condenações penais e crimes"; ou
- quando for especificamente exigido por lei à organização.

Qual o envolvimento do encarregado da proteção de dados?

O encarregado da proteção de dados deve estar integrado em todos os assuntos relacionados com proteção de dados.

Quem pode ser designado encarregado da proteção de dados?

O encarregado da proteção deve possuir conhecimentos especializados no domínio do direito e das práticas de proteção de dados, e revelar a sua capacidade para desempenhar as funções que lhe cabem. Pode ser um empregado da organização ou apenas um prestador de serviços.

Independência do encarregado

O encarregado da proteção deve desempenhar as funções de forma independente:

- não recebe instruções do responsável pelo tratamento;
- não pode ser destituído nem penalizado pelo responsável pelo tratamento;
- não pode exercer outras funções incompatíveis com a de encarregado; e
- comunica diretamente com a direção ao mais alto nível.

Grupos de empresas

Os grupos de empresas podem designar apenas um encarregado da proteção de dados, desde que seja facilmente acessível para cada estabelecimento.

Deveres e funções do encarregado

Deveres de publicidade

Os contactos do encarregado da proteção de dados devem ser divulgados e comunicados à autoridade de controlo.

Obrigação de comunicar os contactos do encarregado

No momento da recolha dos dados o responsável pelo tratamento deve facultar ao titular, entre outras informações, os contactos do encarregado da proteção de dados.

Contacto com os titulares dos dados

Os titulares dos dados podem contactar diretamente o encarregado da proteção e exercer junto deste os direitos previstos no Regulamento.

Quem necessita de nomear um encarregado da proteção de dados?

Todos os responsáveis pelo tratamento de dados sensíveis deverão designar um encarregado da proteção de dados., independentemente do número de trabalhadores.

Funções do encarregado

O Regulamento enumera algumas das funções a desempenhar, das quais destacamos:

- informar e aconselhar o responsável pelo tratamento, incluindo os trabalhadores, a respeito das obrigações em proteção de dados;
- controlar todo o processo em conformidade com a legislação de proteção de dados, incluindo a sensibilização e formação do pessoal implicado nas operações de tratamento de dados;
- cooperar com a autoridade de controlo;
- prestar pareceres sobre a avaliação de impacto sobre a proteção de dados nas situações de implementação de determinado tipo de tratamento suscetível de implicar elevados riscos para o titular dos dados; e
- ser um ponto de contacto para a autoridade de controlo.

Conduta e certificação

Códigos de conduta e certificação

O cumprimento dos deveres decorrentes do Regulamento não é realizado através de uma verificação individual, de cada responsável e subcontratante, pelas autoridades de controlo. O Regulamento prevê a utilização de códigos de conduta e certificação para atestar o cumprimento dos deveres de proteção de dados, concedendo a terceiros a supervisão dessa conformidade.

Quem pode elaborar os códigos de conduta?

Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta. As associações ou outras entidades representantes de categorias de responsáveis pelo tratamento, ou subcontratantes, podem alterar ou aditar esses códigos, desde que, entre outras coisas, abordem:

- o tratamento equitativo e transparente;
- os legítimos interesses dos responsáveis pelo tratamento em contextos específicos;
- a recolha de dados pessoais;
- a pseudonimização dos dados pessoais;
- as informações prestadas às crianças e a sua proteção, e o modo pelo qual o consentimento do titular das responsabilidades parentais da criança deve ser obtido;
- a informação prestada ao público e aos titulares dos dados;
- o exercício dos direitos dos titulares dos dados;
- a transferência de dados pessoais para países terceiros;
- a notificação de violações de dados pessoais às autoridades de controlo, e a comunicação dessas violações de dados pessoais aos titulares dos dados.
- as obrigações gerais dos responsáveis pelo tratamento e as medidas destinadas a garantir a segurança do tratamento; e
- as ações extrajudiciais e outros procedimentos de resolução de litígios entre os responsáveis pelo tratamento e os titulares dos dados relativas ao tratamento.

Controlo e Certificações

Cumprimento do código de conduta

Para além das autoridades de controlo, o cumprimento das disposições dos códigos de conduta, cabem também a um organismo de controlo certificado que demonstre:

- independência e conhecimentos necessários;
- ter estabelecido procedimentos de avaliação de elegibilidade dos responsáveis pelo tratamento e subcontratantes para cumprir o código, verificando o seu respeito e revendo periodicamente o seu funcionamento;
- ter estabelecido procedimentos e estruturas para tratar reclamações relativas a violações do código; e
- não existir um conflito de interesses com as funções e atribuições.

O organismo de controlo pode suspender ou excluir do código o responsável ou subcontratante infrator. Notificando a autoridade de controlo das medidas e fundamentos.

O incumprimento das obrigações do organismo de controlo, implicam a aplicação de coimas até € 10.000.000,00.

Certificações

O Regulamento promove os procedimentos de certificação de conformidade do tratamento dos dados, através do uso de selos e marcas de proteção de dados.

Os responsáveis pelo tratamento ou subcontratantes localizados fora da UE poderão usar esses certificados, selos ou marcas para demonstrarem a conformidade com as disposições do Regulamento.

A certificação será efetuada por um organismo de certificação, devidamente acreditado pelas autoridades de controlo dos Estados-Membros (pelo período de 5 anos) .

A certificação é concedida pelo período máximo de 3 anos (renovável), podendo ser revogada se as condições para a certificação não estiverem a ser cumpridas.

A certificação dos mecanismos não diminui ou exclui as responsabilidades do subcontratante ou do responsável pelo tratamento.

O Comité recolhe todos os procedimentos de certificação, selos e marcas de proteção de dados aprovados num registo e, disponibiliza-os ao público por todos os meios adequados.

Transferência de dados para países terceiros

A transferência de dados

À semelhança da Diretiva de 95 é permitida a transferência de dados para países que demonstrem um nível adequado de proteção de dados.

O Regulamento permite que a decisão de adequação para transferência de dados abranja não só países terceiros, mas também para territórios, organizações internacionais ou setores específicos de um país terceiro.

Regras vinculativas aplicáveis às empresas (*Biding Corporate Rules – BCR)*

O Regulamento prevê a criação de regras vinculativas aplicáveis às empresas como forma apta para a transferência de dados para países terceiros. Estas regras têm de ser aprovadas pelas autoridades de controlo, de acordo com o procedimento de controlo de coerência.

Os grupos de empresas ou os grupos empresariais podem usar regras vinculativas comuns, devidamente aprovadas, para transferirem dados pessoais para empresas do grupo localizadas fora da UE.

As regras vinculativas são um mecanismo bastante versátil devido à sua flexibilidade e a sua carga reduzida administrativa quando implementado.

Derrogações específicas

Tal como na Diretiva de 95 existem situações específicas em que se poderão transferir os dados sem necessidade de obediência a nenhum dos mecanismos previstos. O Regulamento introduz o novo critério geral a ponderar, o dos "interesses legítimos visados pelo responsável pelo seu tratamento".

Os Códigos de conduta enquanto compromissos vinculativos

Os códigos de conduta poderão facilitar a transferência de dados para países terceiros, visto que funcionam como compromissos vinculativos e com força executiva no sentido de aplicar as garantias apropriadas à proteção de dados.

Compete às autoridades de controlo a aprovação dos códigos de conduta novos, alterados ou retificados. Posteriormente, serão registados e publicados.

Se os códigos de conduta versarem sobre o tratamento de dados em diversos Estados-Membros, estes deverão ser submetidos a apreciação do Comité, e em caso de aprovação serão publicados pela Comissão.

A adesão a códigos de conduta aprovados é um elemento demonstrativo do cumprimento do responsável pelo tratamento das suas obrigações.

Portabilidade de Dados e Direito a ser esquecido

Direito a ser esquecido

O Regulamento, à semelhança da decisão do Tribunal de Justiça da EU, prevê o direito a ser esquecido. O titular dos dados tem o direito de solicitar ao responsável pelo tratamento o pagamento dos seus dados sempre que estes sejam publicados.

O responsável pelo tratamento comunica a cada destinatário do tratamento qualquer retificação, ou apagamento dos dados pessoais, ou limitação do tratamento.

Direito à limitação do tratamento

O titular dos dados pode solicitar a limitação do tratamento, devendo o responsável pelo tratamento retirar do sistema de armazenamento geral ou de um site público, de modo a evitar o posterior processamento.

Direito à portabilidade dos Dados

O titular dos dados tem o direito de receber os dados pessoais transmitidos num formato estruturado, de uso corrente e de leitura automática, e que lhe digam respeito. A transmissão tem de ser fundada no consentimento ou por contrato.

A transmissão, se possível, pode ser feita diretamente para outro responsável pelo tratamento.

Direito de acesso do titular dos dados

O Regulamento prevê um direito de acesso mais amplo, os titulares têm direito a uma cópia dos dados em processamento e, ainda a aceder a informações como: os fins do processamento, o período de tempo de armazenamento dos dados, a identidade dos destinatários dos dados, a lógica de processamento automático de dados, e as consequências de qualquer definição de perfis.

Direito de oposição

O Regulamento, ao contrário da Diretiva de 95, possibilita ao titular dos dados opor-se ao tratamento em qualquer momento quando este é fundado no interesse público ou em interesses legítimos do responsável pelo tratamento, a não ser que este apresente razões imperiosas.

Na prática, o titular dos dados terá o direito de levantar o consentimento quando o processamento seja efetuado com esse fundamento.

Desafio para as empresas

É previsível que os responsáveis pelo tratamento venham a necessitar de plataformas de comunicação e apoio ao titular dos dados, pois terão de comunicar de forma concisa, transparente, inteligível e de fácil acesso, sem demora injustificada (no prazo de 1 mês).

Pseudonimização e Coimas

Pseudonimização

O Regulamento define e promove o tratamento dos dados "pseudominizados" de modo a que a ligação a uma pessoa não seja possível, sem recurso a informações adicionais que se encontram separadas das restantes.

Proteção de dados desde a conceção (*Data protection by design*)

O conceito de proteção de dados desde a conceção é formalmente abordada no Regulamento. A proteção deve ser uma característica do desenvolvimento da atividade, em vez de algo efetuado posteriormente.

A Pseudonimização é observada como uma das medidas técnicas e organizativas adequadas para a prossecução de uma proteção desde a sua conceção.

Segurança do tratamento

A pseudonimização e a cifragem dos dados pessoais são observadas como técnicas aptas a promover a segurança dos dados pessoais.

Os códigos de conduta também devem promover a pseudonimização de dados, o emprego presume a adesão aos princípios do Regulamento.

Coimas

O Regulamento é bastante rigoroso quanto à aplicação de coimas. As autoridades nacionais são responsáveis pela sua aplicação pela infração das disposições do Regulamento.

O valor fixado é muito superior ao previsto no quadro legal vigente, as coimas para as empresas poderão atingir € 20.000.000 ou 4% do volume de negócios anual a nível mundial, consoante o valor mais elevado.

Reclamação

A legitimidade para apresentação de queixa estende-se também às associações que considerem existir uma violação dos dados pessoais, independentemente da existência de mandato com o titular dos dados violados.

As autoridades nacionais devem disponibilizar formulários de reclamação em formato eletrónico para facilitarem o acesso a este direito aos cidadãos.

O responsável pelo tratamento dos dados deve indicar, entre outras informações, o direito de reclamar junto da autoridade de controlo.

SOBRE NÓS

A nossa experiência

No mercado global e competitivo dos dias de hoje, a Macedo Vitorino & Associados presta assessoria jurídica a clientes nacionais e estrangeiros em matérias de direito imobiliário e planeamento urbanístico. Estabelecemos relações estreitas de correspondência e parceria com algumas das mais prestigiadas sociedades de advogados internacionais da Europa, dos Estados Unidos e da Ásia, o que nos permite prestar aconselhamento em operações internacionais de forma eficaz.

A Macedo Vitorino & Associados foi recomendada pela publicação "The European Legal 500" pela sua experiência em treze das dezoito áreas analisadas pelo directório internacional, nomeadamente em “Banking and Finance”, “Capital Markets”, “Project Finance”, “Tax”, “Real Estate”, “Telecoms” and “Litigation”.

A actuação da Macedo Vitorino & Associados é ainda destacada pela IFLR 1000 em todas as áreas analisadas em Portugal, nomeadamente em “Project Finance”, “Corporate Finance” e “Mergers and Acquisitions”. A Chambers and Partners destaca a Macedo Vitorino & Associados em “Banking”, “Corporate” e “Litigation”, entre outras áreas.

O nosso grupo de Telecomunicações tem elevada experiência em diversas áreas, incluindo:

- Proteção de dados
- Tecnologia da Informação (TI)
- Licenciamento e Regulamentação
- Direito da União Europeia e da Concorrência
- Contratos de cliente
- Contratos de compra de bens online
- Interconexão
- Construção de redes de Telecomunicações e Contratos de Manutenção

Se quer saber mais sobre a Macedo Vitorino & Associados por favor visite o nosso site em www.macedovitorino.com

João Macedo Vitorino
jvitorino@macedovitorino.com

Rua do Alecrim 26E | 1200-018 Lisboa | Portugal
Tel.: +351 213 241 900 | Fax: +351 213 241 929
www.macedovitorino.com