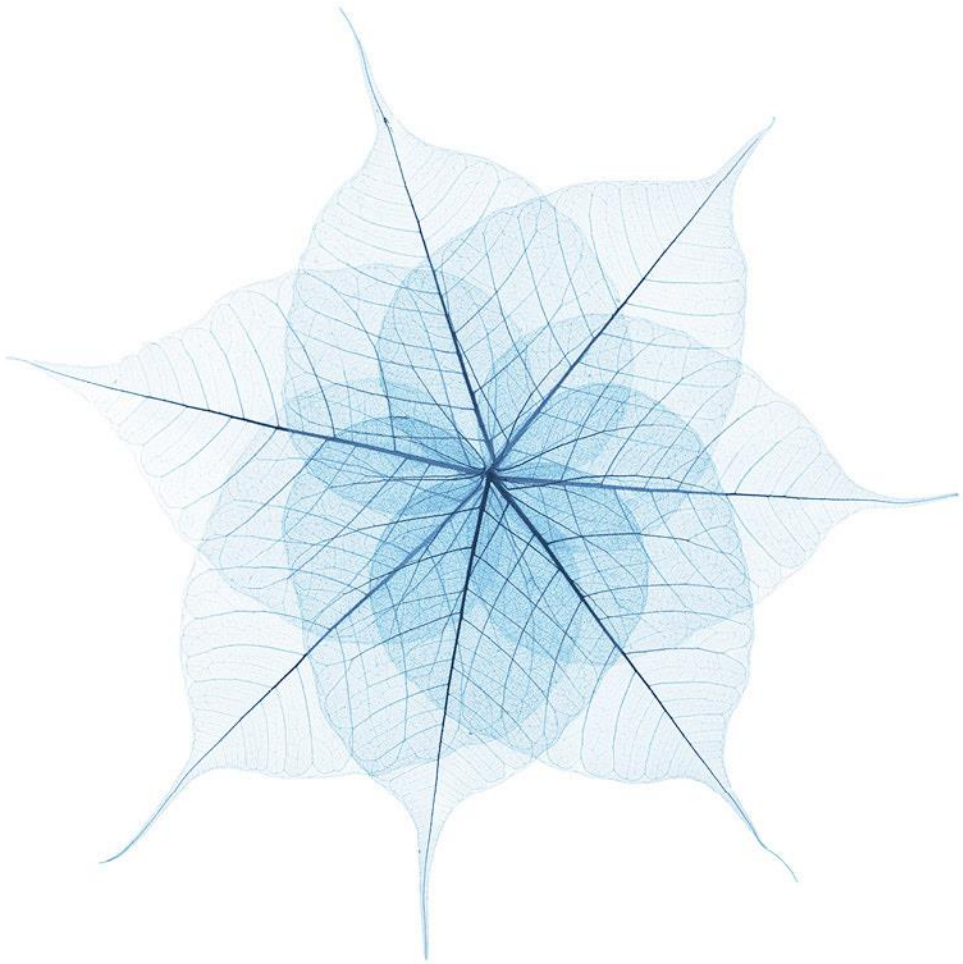
Proteção de Dados

João Paulo Mioludo



- A PROTEÇÃO DAS PESSOAS SINGULARES NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS E À LIVRE CIRCULAÇÃO DESSES DADOS

- REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS

- **Recomendação nº 73(22)** – Comité de Ministros do Conselho da Europa (26 de setembro de 1973)

  Proteção da vida privada das pessoas singulares face aos bancos de dados eletrónicos no setor privado

- **Convenção nº 108** – Comité de Ministros do Conselho da Europa (28 de janeiro de 1981) – Ratificado Decreto PR nº 21/93, de 9 de julho

  Proteção das pessoas relativamente ao tratamento automatizado de dados pessoais

Constituição de 1976 – art. 35º

- Consagra o direito de informação e atualização
- Proíbe em absoluto o tratamento relativo a alguns dados sensíveis
- Acórdão do Tribunal Constitucional de 01.02.1989

  Inconstitucionalidade por omissão

  Legislação sobre tratamento automatizado de dados pessoais

Diretiva 95/46/CE do Parlamento e do Conselho – 24.10.1995

- **Cons. 2º** - "Os sistemas de tratamento de dados devem respeitar as liberdades e os direitos fundamentais das pessoas singulares e contribuir para o progresso económico e social, o desenvolvimento económico e o bem-estar dos indivíduos"

- **Cons. 3º** - "Numa perspetiva de desenvolvimento do mercado interno reconhece-se ser primordial assegurar a livre circulação de dados pessoais nos Estados-membros como corolário lógico da livre circulação de mercadorias, de pessoas, dos serviços e de capitais"

Constituição de 1976 (art. 35º) – Legislação ordinária

- 4ª revisão constitucional – Lei Constitucional nº 1/97, de 20 de setembro

- Nova lei sobre proteção de dados (revogadas as Leis nº 10/91, de 29 de abril, e nº 28/94, de 29 de agosto)

- *[Diretiva 97/66/CE – tratamento de dados pessoais e proteção da privacidade no setor das telecomunicações – Lei nº 69/98, de 28 de outubro]*

Constituição de 1976 – art. 35º

- Princípio da autodeterminação informacional
- Entidade administrativa independente – atribuição genérica de garantir a proteção de dados pessoais tratados automaticamente
- Interconexão de ficheiros

  Processamento e relacionamento de informação – sociedade da informação
- Dados sensíveis
- Ficheiros manuais

Lei nº 67/98, de 23 de outubro - Lei de Proteção de Dados Pessoais

- Princípio geral – transparência (art. 2º)
- Âmbito de aplicação (art. 4º, nº 1)
- Exceção: atividades exclusivamente pessoais ou domésticas (art. 4º, nº 2)

  [Ficheiros instalados em empresas]

- Videovigilância (art. 4º, nº 4)

Comissão Nacional de Proteção de Dados

- Emissão de pareceres
- Decisão
- Poder regulamentar
- Investigação
- Outros

Legitimidade para o tratamento de dados

A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização (art. 35º, nº 2 CRP)

Regimes diferenciados:

- Dados sensíveis
- Atividades ilícitas, infrações penais e contraordenações
- Outras categorias de dados

Tratamento de dados sensíveis

– Convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, saúde, vida sexual e dados genéticos

- É proibido o tratamento (princípio geral)
- Tratamento estabelecido por lei
- Consentimento expresso dos titulares – garantias
  - *[Anonimização]*

Qualidade dos dados

– Princípio da transparência

Ac. TJ de 06.10.2015 – “safe harbour”

Nossa “Meet the Law” de 12.10.2015

- Recolha de dados
- Atualização e conservação dos dados
- Direito de informação, acesso e retificação

Procedimentos junto da CNPD

- Obrigação de notificação pelas entidades responsáveis, antes do tratamento

- Controlo e legalização dos tratamentos

  – Consulta / emissão de pareceres

  – Controlo prévio – autorizações

  – Transferência de dados

  – Registo

Incumprimento

- Tutela administrativa e jurisdicional

  Reparação por prejuízos sofridos

- Medidas sancionatórias

- Interrupção ou destruição de ficheiros

Regulamento Geral sobre a Proteção de Dados na União Europeia

– Regulamento UE 2016/679

João Leitão Figueiredo

Introdução

- Ao publicar o projeto de Regulamento Geral sobre a Proteção de Dados em janeiro de 2012, a Comissão Europeia deu início a 4 anos de discussões, negociações e lobbies, como poucas vezes a União Europeia (UE) foi confrontada.

- As alterações finalmente aprovadas e que produzirão efeitos apenas em Maio de 2018 são substanciais e ambiciosas. O Regulamento, compreendendo quase 100 páginas, constitui uma das mais amplas peças legislativas aprovada pela UE nos últimos anos e os conceitos introduzidos, como o "direito a ser esquecido", a portabilidade dos dados, a notificação de violação de dados e a prestação de contas (nomeando apenas algumas novidades) implicarão uma necessidade de adaptação que se prevê delicada e morosa.

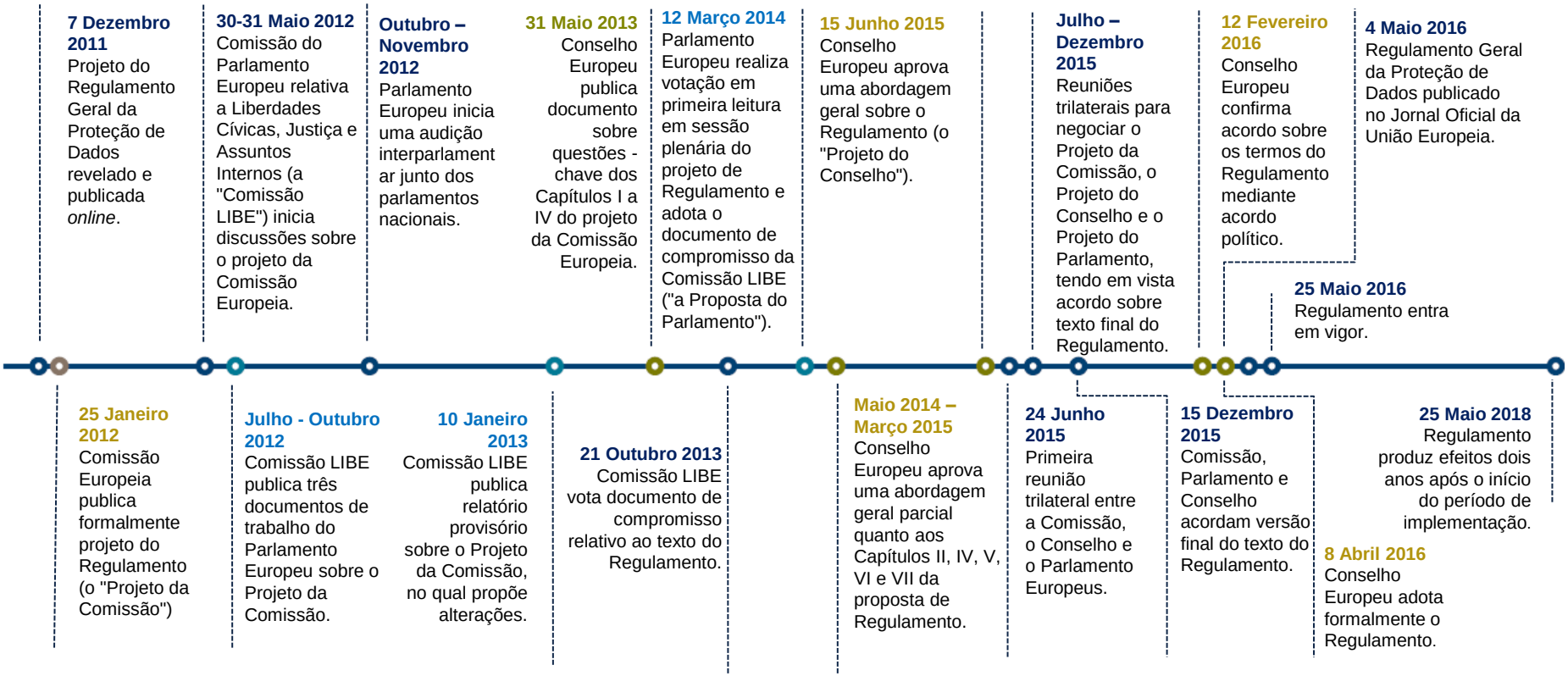
- Salientamos que a própria natureza do diploma - um Regulamento e não uma Diretiva – implica que o RGPD constitua uma novidade em toda a plenitude, inclusive no modelo legislativo adotado.

- A presente apresentação, pela sua natureza, não poderá abordar a totalidade das temáticas ou apresentar o nível de detalhe técnico de que o Regulamento é merecedor, esperamos, contudo, que a mesma permita estimular todos os presentes a enfrentar de forma mais informada e preparada os desafios que se avizinham.

Sumário

- Cronograma
- Âmbito Material;
- Âmbito Territorial;
- Conceitos e Princípios;
- Direitos do Titular dos Dados;
- Responsabilidade, Segurança e Notificação de Violação de Dados;
- Transferência de Dados;
- Reguladores;
- Enforcement;
- Limitações e Casos Especiais.

Cronograma


7 Dezembro 2011
Projeto do Regulamento Geral da Proteção de Dados revelado e publicada *online*.
30-31 Maio 2012
Comissão do Parlamento Europeu relativa a Liberdades Cívicas, Justiça e Assuntos Internos (a "Comissão LIBE") inicia discussões sobre o projeto da Comissão Europeia.
Outubro – Novembro 2012
Parlamento Europeu inicia uma audição interparlamentar junto dos parlamentos nacionais.
31 Maio 2013
Conselho Europeu publica documento sobre questões - chave dos Capítulos I a IV do projeto da Comissão Europeia.
12 Março 2014
Parlamento Europeu realiza votação em primeira leitura em sessão plenária do projeto de Regulamento e adota o documento de compromisso da Comissão LIBE ("a Proposta do Parlamento").
15 Junho 2015
Conselho Europeu aprova uma abordagem geral sobre o Regulamento (o "Projeto do Conselho").
Julho – Dezembro 2015
Reuniões trilaterais para negociar o Projeto da Comissão, o Projeto do Conselho e o Projeto do Parlamento, tendo em vista acordo sobre texto final do Regulamento.
12 Fevereiro 2016
Conselho Europeu confirma acordo sobre os termos do Regulamento mediante acordo político.
4 Maio 2016
Regulamento Geral da Proteção de Dados publicado no Jornal Oficial da União Europeia.
25 Maio 2016
Regulamento entra em vigor.
25 Janeiro 2012
Comissão Europeia publica formalmente projeto do Regulamento (o "Projeto da Comissão")
Julho - Outubro 2012
Comissão LIBE publica três documentos de trabalho do Parlamento Europeu sobre o Projeto da Comissão.
10 Janeiro 2013
Comissão LIBE publica relatório provisório sobre o Projeto da Comissão, no qual propõe alterações.
21 Outubro 2013
Comissão LIBE vota documento de compromisso relativo ao texto do Regulamento.
Maio 2014 – Março 2015
Conselho Europeu aprova uma abordagem geral parcial quanto aos Capítulos II, IV, V, VI e VII da proposta de Regulamento.
24 Junho 2015
Primeira reunião trilateral entre a Comissão, o Conselho e o Parlamento Europeus.
15 Dezembro 2015
Comissão, Parlamento e Conselho acordam versão final do texto do Regulamento.
25 Maio 2018
Regulamento produz efeitos dois anos após o início do período de implementação.
8 Abril 2016
Conselho Europeu adota formalmente o Regulamento.
Publicações da Comissão Europeia
Publicações do Parlamento Europeu
Publicações do Conselho Europeu

Âmbito Material e Territorial

– O Regulamento, em comparação com a Diretiva 95/46/CE ("Diretiva de Proteção de Dados"), que vem substituir, manifestamente visa proceder a um alargamento do alcance da lei de proteção de dados da UE.

  - Os responsáveis pelo tratamento de dados ou os subcontratantes com sede na UE encontram-se abrangidos pelo âmbito de aplicação do Regulamento – quando sejam tratados dados pessoais, no contexto das suas atividades, independentemente do tratamento ser efetuado dentro ou fora da União.
  - Nos casos em que não exista uma presença na UE, o Regulamento ainda assim se aplicará sempre que: (1) sejam tratados dados pessoais de um residente na UE em conexão com bens ou serviços oferecidos ao mesmo; ou, (2) quando os comportamentos dos titulares dos dados sejam “controlados” no seio da UE.

– Pese embora seja um regulamento, o Regulamento permite aos Estados-Membros legislar em diversas áreas, realidade que, em nosso entender, vai desafiar o objetivo de consistência do Regulamento.

– O Regulamento não se aplica ao tratamento de dados pessoais: (1) efetuado no exercício de atividades não sujeitas à aplicação do direito da União; (2) efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; (3) efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; (4) efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Âmbito Territorial

- Responsáveis e Subcontratantes estabelecidos na UE;
- Responsáveis e Subcontratantes não estabelecidos na UE.

Âmbito Territorial

Responsáveis ou Subcontratantes estabelecidos na UE

O Regulamento será aplicável a entidades com "estabelecimento" na UE, quando dados pessoais sejam tratados "no contexto das atividades" desse estabelecimento.

Caso o pressuposto de aplicação referido seja confirmado, o Regulamento aplica-se independentemente do efetivo processamento de dados ser efetuado, ou não, na UE.

O conceito de “Estabelecimento" foi definido pelo Tribunal de Justiça da União Europeia ("TJUE") no Caso Weltimmo v Naih (C-230/14) de 2015. “Estabelecimento” foi qualificado como um “amplo” e “flexível” conceito, que não deve depender de um específico formato legal, podendo uma entidade estar "estabelecida" onde exerça "qualquer atividade real e efetiva – ainda que mínima” - através de "acordos estáveis" na UE. A mera presença de um representante poderá ser o suficiente.

As entidades que tenham escritórios na UE através dos quais promovam, publicitem ou vendam produtos ou serviços a residentes na UE, serão provavelmente sujeitas ao Regulamento, na medida em que o tratamento de dados pessoais é qualificado como “intimamente ligado” ao estabelecimento e realizado no contexto da atividade desse estabelecimento [Caso Google Spain SL e Google Inc. v AEPD, Mario González Costeja (C-131/12)].

As disposições do Regulamento são diretamente aplicáveis não apenas aos Estados-Membros da UE, mas a todos os países do Espaço Económico Europeu (EEE), como sejam a Islândia, o Liechtenstein e a Noruega.

Âmbito Territorial

Responsáveis ou Subcontratantes não estabelecidos na UE

As entidades estabelecidas fora da UE apenas serão sujeitas ao disposto no Regulamento, quando procedam ao tratamento de dados pessoais de residentes na UE relacionados com:

i. a "oferta de bens ou serviços" (não sendo o pagamento condição necessária para aplicação); ou,

ii. o “controlo” dos comportamentos dos residentes no seio da UE.

A mera possibilidade de acesso a um site a partir da UE não é qualificada como juridicamente relevante. Deve ser evidente que a entidade “considera" que as atividades são direcionadas a residentes na UE.

Endereços de contacto acessíveis a partir da UE ou o uso de um idioma utilizado no país de origem do responsável também não são qualificados como juridicamente suficientes. No entanto, a utilização de uma língua e moeda da UE, a possibilidade de fazer pedidos nesse outro idioma e as referências a usuários ou clientes na UE já serão juridicamente relevantes para aplicação do Regulamento.

Âmbito Territorial

O TJUE, pese embora num contexto distinto [ou seja, ao abrigo do regulamento "Bruxelas 1" (44/2001/CE), que regulamenta a "jurisdição ... em matéria civil e comercial"], já decidiu quando uma atividade (como a oferta de bens e serviços) poderá ser considerada como "dirigida a" Estados-Membros da UE.

As decisões do TJUE constituem um importante auxílio na interpretação do Regulamento, na medida em que, segundo entendimento jurisprudencial, a intenção de segmentar os clientes da UE pode ser ilustrada por:

(1) "Evidências flagrantes", tais como o pagamento de quantias a um motor de busca para facilitar o acesso dos residentes de um Estado-Membro ou onde os Estados-Membros pretendidos sejam designados pelo nome; e,

(2) Outros fatores - eventualmente em combinação - o "carácter internacional" da atividade relevante (por exemplo, atividades turísticas), menções de números de telefone com um código internacional, o uso de um nome de domínio de primeiro nível distinto do existente no país de origem do responsável (como sejam .pt ou .eu), a descrição de "itinerários ... dos Estados Unidos para o lugar onde o serviço é prestado", ou a menção a uma "clientela internacional constituída por clientes domiciliados em vários Estados-Membros". Esta lista não é exaustiva e a questão deve ser determinada casuisticamente, cfr. Caso Pammer v Reederei Karl Schlüter GmbH & Co. e Caso Alpenhof v Heller (Casos apensados C-585/08 e C-144/09).

Âmbito Territorial

O conceito de “Controlo" especificamente inclui o rastreamento de pessoas *on-line* para criação de perfis, em particular quando seja utilizado para tomada de decisões de análise ou previsão de preferências pessoais, comportamentos e atitudes.

As entidades sujeitas ao âmbito de aplicação do Regulamento devem nomear um representante a nível da UE.

Nos termos da Diretiva de Proteção de Dados, as entidades que tinham como alvo titulares de dados residentes na UE, apenas tinham de cumprir as regras da UE se fizessem uso de "equipamento" sito na UE para processar dados pessoais. A referida particularidade impeliu as autoridades de supervisão nacionais, que procuravam afirmar a sua jurisdição, a desenvolver argumentos de que a colocação de cookies ou o pedido de preenchimento formulários por parte dos utilizadores, seria equivalente à utilização de "equipamento" na UE.

Com a implementação do Regulamento a demonstração da aplicabilidade da legislação será, em princípio, mais simples, contudo, admitimos que, nos casos em que as entidades não tenham presença na UE, novas questões de difícil resolução possam surgir.

Conceitos e Princípios

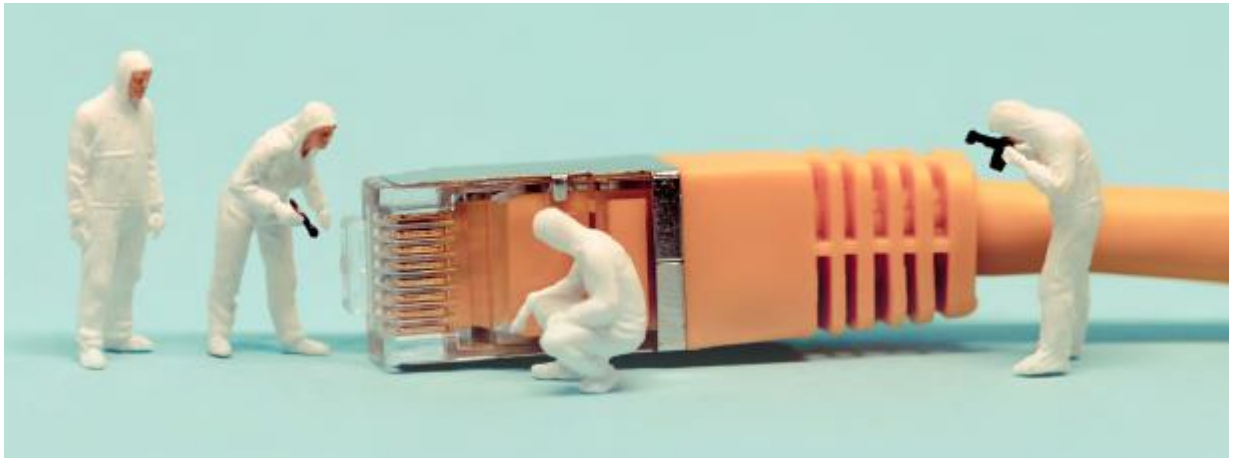
O Regulamento introduzirá relevantes alterações conceptuais e, bem assim, atualizará diversos conceitos atualmente existentes, nomeadamente:

- Transparência e Consentimento;

- Crianças e Consentimento;

- Dados Regulados;

- Pseudonimização.



Princípios

O tratamento de dados, nos termos do Regulamento, deverá orientar-se pelos seguintes princípios (artigo 5º):

- Licitude, Lealdade e Transparência;
- Limitação das Finalidades (definição em virtude dos objetivos);
- Adequação (minimização de dados);
- Limitação da Conservação;
- Integridade e Confidencialidade; e,
- Responsabilidade.

Transparência

O conceito de transparência nos termos do Regulamento apresenta-se numa dupla vertente, por um lado, constitui um dos princípios basilares do tratamento de dados, por outro, impõe um extenso conjunto de deveres de informação (ou à prestação de informação) por parte dos Responsáveis pelo tratamento de dados.

A obrigação de transparência poderá ser sintetizada através dos deveres de informação sobre:

- Identidade e dados de contacto do Responsável;
- Objetivos do tratamento de dados;
- Destinatários (ou categorias de destinatários);
- Detalhes sobre a transferência de dados para fora da EU (ou EEE);
- Período de conservação de dados;
- Direito de Acesso, Retificação, Portabilidade, Apagamento ou Limitação;
- Direito a apresentação de reclamação;
- Existência de decisões automatizadas, incluindo a definição de perfis.

Consentimento

O artigo 7º do Regulamento introduz alterações assinaláveis ao conceito de consentimento, nomeadamente que o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.

O consentimento do titular dos dados deverá ser uma manifestação de vontade livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

Caso o consentimento do titular dos dados seja dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente dos demais assuntos de modo inteligível, acessível e numa linguagem clara e simples. A presente regra deriva do Considerando 42 da Diretiva 93/13/CEE (Cláusulas Abusivas).

O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, contudo a retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado.

É introduzida ainda da obrigatoriedade de verificação se a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não seja necessário para a execução desse contrato. Nos casos em que tal necessidade não se verifique, o consentimento não será considerado válido.

Crianças

A importância da proteção das crianças é mencionada múltiplas vezes no Regulamento, contudo, é oferecida uma frágil harmonização no texto final, pelo que admitimos que as restrições substantivas, provavelmente, apenas resultarão de leis nacionais ou códigos de conduta.

O Artigo 8 do Regulamento constitui a principal disposição relativa a crianças, o qual exige que o consentimento dos pais deve ser obtido, no que respeita à oferta direta de serviços da sociedade da informação, quando as crianças tenham menos 16 anos. O referido limite de idade poderá, por opção dos Estados-Membros ser reduzida para os 13 anos de idade.

O Responsável é também obrigado, nos termos do Artigo 8 (2) do Regulamento, a realizar esforços "esforços razoáveis“, tendo em conta tecnologia disponível, para verificar se o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança .

A presente norma só afecta determinados dados online – os dados off-line continuam a ser sujeitos às regras dos Estados-Membros sobre a capacidade de consentir.

As informações remetidas a crianças deverão, nos termos do artigo 12 do Regulamento, utilizar uma linguagem clara e simples, sem prejuízo da obrigação de utilização de uma forma concisa, transparente, inteligível e de fácil acesso.

Dados Regulados

Dados Pessoais e Dados Sensíveis

O Regulamento é aplicável a todos os dados a partir do quais um indivíduo possa ser identificado ou identificável, direta ou indiretamente. O pressuposto de Diretiva “todos os meios razoavelmente suscetíveis de serem utilizados" para a identificação é mantido.

Nos Considerandos são ainda destacadas certas categorias de dados *online* que podem ser qualificados como pessoais, por exemplo, identificadores *online*, identificadores de dispositivos, IDs de cookies e endereços IP.

"Categorias Especiais de Dados" (Dados Sensíveis) são mantidos e aprofundados - para cobrir os dados genéticos e dados biométricos. Tal como acontece com a atual Diretiva de Proteção de Dados, o processamento destes dados está sujeito a condições mais rigorosas do que outros tipos de dados pessoais.

Pseudonimização

Constitui uma técnica de tratamento de dados pessoais, em moldes em que já não possam ser relacionados com um "sujeito de dados" específico sem a utilização de informação adicional, devendo por isso os conjuntos de informação ser conservados separadamente e sujeitos a medidas técnicas e organizacionais para garantir a ausência de relação.

A “Informação Pseudonimizada” constitui ainda um dado pessoal.

A utilização da pseudonimização é incentivada quando, por exemplo:

• Se determina que o processamento é "incompatível" com as finalidades para as quais os dados pessoais foram originalmente recolhidos e tratados;

• Constitui uma técnica para satisfazer as necessidades de implementação de “políticas de privacidade por conceção ou por defeito";

• Contribui para o cumprimento das obrigações de segurança de dados do Regulamento; e

• As entidades desejem utilizar dados pessoais para a pesquisas históricas ou científicas ou para fins estatísticos.

Direitos do Titular dos Dados

- Direito à Prestação de Informação;
- Direitos de Acesso, Retificação e Portabilidade dos Dados;
- Direito de Oposição; e,
- Direito ao apagamento dos dados («direito a ser esquecido») e Direito à Limitação do Tratamento.

Direito à Prestação de Informação

Os Responsáveis pelo tratamento de dados devem fornecer informação aos titulares dos dados de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças, de modo a garantir a transparência do tratamento.

Direitos de Acesso, Retificação e Portabilidade dos Dados

O Direito de Acesso impõe aos responsáveis pelo tratamento a obrigação de, a pedido dos titulares dos dados:

- Confirmar se tratam dados pessoais de um determinado titular, as finalidades do tratamento, tipos de dados tratados, destinatários e prazos de conservação;

- Fornecer uma cópia dos dados pessoais em formato eletrónico comummente utilizado; e

- Fornecer informações detalhadas por escrito.

Os titulares dos dados podem requerer que os seus dados pessoais sejam remetidos, diretamente ou para um novo prestador de serviços, mediante formato legível por máquina, se os dados em questão foram: 1) fornecidos pelo titular ao responsável; 2) sejam tratados automaticamente; e 3) o tratamento seja efetuado com base no consentimento ou no cumprimento de um contrato.

A solicitação deve ser atendida no prazo de um mês (com extensões em casos legalmente considerados) e qualquer intenção de não cumprimento deve ser explicada ao titular dos dados.

O direito de acesso é destinado a permitir que os titulares verifiquem a legalidade do tratamento efetuado e exerçam o direito de retificação ou solicitem uma cópia da mesma quando esta não seja suscetível de prejudicar direitos de terceiros.

Direito de Oposição

O Direito de Oposição permite aos Titulares dos Dados oporem-se à utilização dos seus dados quanto a determinados tipos específicos de tratamento, como, por exemplo:

- Marketing direto;

- Tratamento necessário ao exercício de funções de interesse público ou necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros ; e,

- Tratamento para fins estatísticos ou de investigação.

Apenas o direito de oposição ao marketing direto é absoluto (isto é, sem necessidade de demonstração dos fundamentos de objeção), não compreendendo qualquer excepção que permita a continuação do tratamento de dados.

Os Responsáveis têm a obrigação de informar os titulares dos dados, numa fase preliminar, de forma clara e independente de outras obrigações de informação, sobre os seus direitos.

A prestação de serviços *on-line* deve oferecer um método automatizado para o exercício do direito de oposição.

Direito ao apagamento dos dados («direito a ser esquecido»)

O Regulamento introduziu direitos mais extensos e imprecisos, como o direito a ser esquecido (agora denominado de direito ao apagamento dos dados) e o direito à limitação do tratamento.

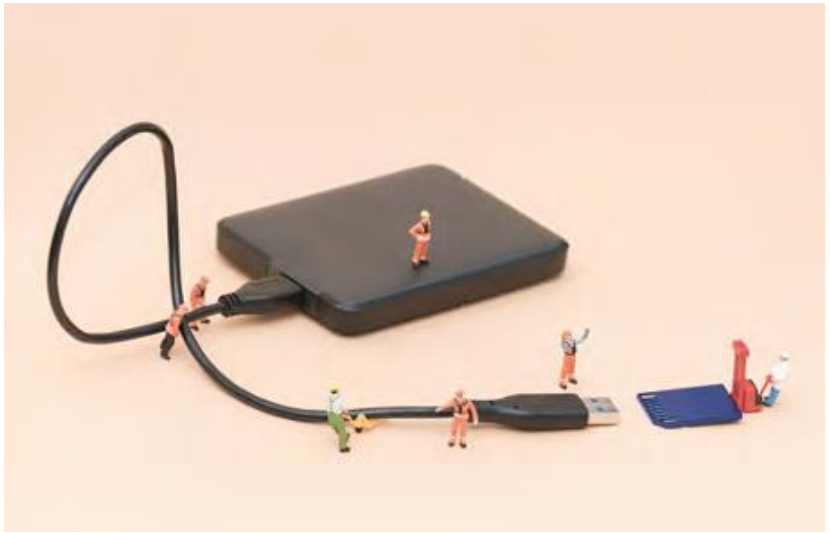
Em concreto, são conferidos aos titulares direitos de requerer que os seus dados sejam "apagados" quando exista, ou se considere que exista, um problema com a legalidade subjacente ao tratamento, quando os titulares revoguem o seu consentimento ou quando os dados deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento.

O titular pode também exigir que o responsável 'restrinja' o tratamento dos seus dados enquanto estiver pendente uma reclamação sobre a exatidão dos dados, ou quando subsistam dúvidas sobre a licitude do tratamento mas o titular se oponha ao “apagamento” e requeira a mera limitação.

Os Responsáveis que tornaram públicos dados que foram alvo do exercício do direito ao apagamento dos dados, encontram-se obrigado a notificar outros Responsáveis ou Subcontratantes de tal exercício do direito, dos seus termos e condições. Esta é uma nova obrigação ampla e desafiante.

Responsabilidade, Segurança e Notificação de Violação de Dados

- Proteção de Dados por Defeito;
- Avaliação de Impacto sobre a Proteção de Dados;
- Encarregado da Proteção de Dados;
- Subcontratantes;
- Notificação de Violação de Dados;
- Requisitos de Documentação;
- Códigos de Conduta e Certificações.



Proteção de Dados por Defeito

As entidades devem implementar medidas técnicas e organizativas para demonstrar o adequado cumprimento das regras relativas ao tratamento de dados impostas pelo Regulamento (cfr. artigo 25º do Regulamento).

A adoção de políticas de pessoal adequadas é especificamente mencionada, como é o uso de pseudónimos (para garantir a conformidade com as obrigações de minimização de dados)

Avaliação de Impacto sobre a Proteção de Dados

A Avaliação de Impacto sobre a Proteção de Dados (ou PIA – Privacy Impact Assessments) consiste numa avaliação para identificar e minimizar os riscos de não conformidade. O conceito não é novo – as orientações atuais já recomendam o seu uso - mas o Regulamento formaliza a sua execução como requisito.

Especificamente, os Responsáveis pelo Tratamento devem assegurar que a PIA foi executada em qualquer atividade de tratamento de “alto risco” antes de ser iniciada - medida por referência ao risco de violação dos direitos e liberdades das pessoas singulares.

O tratamento "em larga escala" de dados sensíveis, ou a criação de perfis são citados como exemplos (não exaustivos) de tratamentos de alto risco. As autoridades de controlo estão a publicar detalhes de mais exemplos e orientações.

O Regulamento impõe que uma PIA inclua, no mínimo:

• Uma descrição das atividades de tratamento de dados e sua finalidade;

• Uma avaliação da necessidade e proporcionalidade do tratamento, os riscos decorrentes e as medidas adotadas para mitigar esses riscos, em particular garantias e medidas de segurança para proteger os dados pessoais e o respeito pelo Regulamento.

Encarregado da Proteção de Dados

Os Reponsáveis e Subcontratantes são livres de designar um Encarregado da Proteção de Dados (DPO), mas os seguintes são obrigados a fazê-lo:

- As autoridades públicas (com algumas pequenas excepções);
- Qualquer organização cuja atividade requeira:
  - "Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares"; ou,
  - Processamento de "grande escala" de dados sensíveis ou registos criminais;
- Quando obrigados por lei nacional (Alemanha).

Os Encarregados devem ser selecionados em função das suas qualidades profissionais e conhecimento especializado (o empregador é obrigado a auxiliar o Encarregado a manter o nível de conhecimento).

As tarefas do Encarregado deverão incluir, no mínimo: aconselhamento dos seus colegas e controlo do cumprimento do Regulamento, da Lei da Proteção de Dados, das políticas de privacidade e dos códigos de conduta da entidade empregadora, formação e sensibilização, execução de auditorias e cooperação com as autoridades de controlo.

As entidades devem garantir que o Encarregado dispõe de recursos adequados para o cumprimento das suas obrigações de acordo com o Regulamento, devendo o Encarregado reportar diretamente ao mais alto cargo de gestão.

As empresas pertencentes a um único grupo económico podem nomear um único Encarregado. O Encarregado pode ser um empregado ou um subcontratado.

Transferência de Dados

As transferências de dados pessoais para destinatários em "países terceiros" [ou seja, fora do Espaço Económico Europeu ("EEE")] continuam a ser reguladas e restritas em determinadas circunstâncias.

As obrigações implementadas pelo Regulamento são muito semelhantes às impostas pela Diretiva, com algumas melhorias nos mecanismos de cumprimento disponíveis, nomeadamente a remoção da necessidade de notificar as cláusulas contratuais tipo às autoridades de controlo e o incentivo ao desenvolvimento de códigos de conduta de transferência adequados e a certificação de modelos operacionais.

O cumprimento de regras de transferência de dados continuará a ser um problema significativo, não apenas para as organizações multinacionais, mas também para as empresas que utilizam cadeias de fornecimento que processem dados pessoais fora do EEE.

A violação das disposições do Regulamento relativas à transferência de dados será tratada no capítulo das coimas, contudo salientamos, desde já, a possibilidade de imposição de coimas até 4% do volume de negócios anual a nível mundial.

O processo de não-conformidade poderá ser iniciado contra Responsáveis pelo Tratamento e Subcontratantes.

Subcontratantes

O Regulamento impõe um especial dever de cuidado aos Responsáveis pelo Tratamento na seleção dos seus prestadores de serviços de tratamento de dados pessoais, exigindo que a documentação dos procedimentos de adjudicação e documentos de concurso sejam regularmente avaliados.

Os contratos com os prestadores de serviços devem obrigatoriamente incluir um conjunto de cláusulas referentes, por exemplo, identificação dos dados tratados e ao período de conservação, medidas de segurança a implementar, mecanismos de assistência técnica em caso de falha ou violação de segurança, pseudonimização, medidas de criptografia e obrigações de assistência em auditorias.

As referidas obrigações são, do mesmo modo, aplicáveis aos contratos celebrados entre Subcontratantes e terceiros subcontratantes.

A Comissão e as autoridades de controlo deverão, futuramente, publicar formulários com cláusulas contratuais pré-aprovadas, tendo em vista a clarificação dos aspetos mencionados.

As alterações previstas pelo Regulamento implicarão, necessariamente uma alteração nas práticas comerciais atualmente existentes, fazendo impender sobre os Subcontratantes um conjunto de obrigações adicionais tendo em vista o combate a abordagens puramente economicistas.

Notificação de Violação de Dados

No caso de um incidente que possa ser enquadrado como uma violação da segurança que provoque a destruição acidental ou ilícita, a perda, a divulgação não autorizada ou o acesso a dados pessoais transmitidos, armazenados ou de outro modo processados, o novo regime de notificação de violação do Regulamento impõe um conjunto de obrigações diferenciadas:

i. Obrigações dos Subcontratantes perante os Responsáveis pelo Tratamento;
ii. Obrigações dos Responsáveis perante as Autoridades de Controlo; e,
iii. Obrigações dos Responsáveis perante os Titulares dos Dados.

Notificação de Violação de Dados

Obrigações dos Subcontratantes perante os Responsáveis pelo Tratamento

Prazo:

Sem demora injustificada, após tomada de conhecimento.

Exceções:

Não se encontram legalmente previstas.

Observações:

Todas as violações terão de ser notificadas.

O Comité deverá aprovar orientações para clarificar a noção de “demora injustificada" e as circunstâncias particulares em que um Subcontratante é obrigado a notificar a violação de dados pessoais.

Notificação de Violação de Dados

Obrigações dos Responsáveis perante as Autoridades de Controlo

Prazo:

Sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma.

Exceções:

Não se encontram legalmente previstas.

Observações:

Quando os prazos de notificação não possam fundadamente ser respeitados, o Responsável deverá apresentar à Autoridade de Controlo os motivos justificativos (por exemplo, um pedido de uma autoridade policial).

O Comité deverá aprovar orientações para clarificar a noção de “demora injustificada" e as circunstâncias particulares em que um Responsável é obrigado a notificar a violação de dados pessoais.

Notificação de Violação de Dados

Obrigações dos Responsáveis perante os titulares dos dados

Prazo:

Sem demora injustificada. A necessidade de atenuar um risco imediato implicará uma comunicação imediata dirigida aos titulares dos dados, enquanto que a necessidade de implementar medidas adequadas contra a continuação ou ocorrência de violações de dados semelhantes pode justificar a prorrogação do prazo de comunicação.

Exceções:

A notificação de violação de dados não será devida quando:

- Seja provável que da violação não resulte um elevado risco para os direitos e liberdades dos titulares em causa;

- Protecções técnicas e organizativas adequadas estavam em funcionamento no momento do incidente (por exemplo, existência de dados criptografados); ou,

- Implique esforços desproporcionados, devendo então ser feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados sejam informados de forma igualmente eficaz.

Documentação

Os Responsáveis pelo tratamento são obrigados a efetuar Registo Interno de Violação de Dados Pessoais para cada incidente "que compreende os factos relacionados com a violação dos dados pessoais, os seus efeitos e as medidas correctivas tomadas". A autoridade de controlo pode ser “convidada” a avaliar o cumprimento das obrigações de notificação de violação de dados dos Responsáveis.

O Regulamento prevê também requisitos para a comunicação de incidentes: (A) à autoridade de controlo (por exemplo, descrição da natureza da violação de dados pessoais, incluindo, quando possível, as categorias e número aproximado de pessoas afetadas e as categorias e número aproximado de registos de dados afetados, entre outros); e (B) aos titulares de dados (por exemplo, descrição em linguagem clara e simples da natureza da violação de dados pessoais e prestação, pelo menos, das seguintes informações: (i) o nome e os dados de contacto do responsável pela protecção de dados ou outro ponto de contacto onde mais informações podem ser obtidas; (ii) as prováveis consequências da violação de dados pessoais, e (iii) as medidas tomadas ou propostas pelo subcontratado para resolver o incidente, incluindo, se for caso disso, medidas para mitigar possíveis efeitos adversos).

Código de Conduta

Os Códigos de Conduta constituem um importante componente na ampliação e adaptação das ferramentas para o cumprimento das obrigações de protecção de dados a que os Responsáveis e Subcontratantes podem recorrer.

Os Códigos deverão compreender orientações específicas em determinadas áreas-chave, incluindo:

- interesse legítimo em contextos específicos;
- pseudonimização;
- exercício de direitos pelo titular dos dados;
- protecção dos menores e modos de consentimento dos pais;
- a correcta aplicação da política de proteção de dados desde a conceção e por defeito, e as medidas de segurança;
- notificação de violações de segurança; e
- resolução de conflitos entre o responsável e titular dos dados.

Os Códigos deverão ser disponibilizados ao público e permanecer acessíveis para consulta.

A verificação da implementação e cumprimento das regras constantes dos Códigos de Conduta, apenas poderá ser efetuada por entidades independentes e acreditadas pela autoridade de controlo competente.

Certificação

O conceito de certificação do tratamento de dados é um desenvolvimento significativo na criação de um quadro confiável e auditável para operações de processamento de dados. É provável que seja particularmente relevante no contexto da *cloud computing* e de outros serviços partilhados, em que as auditorias individuais não são muitas vezes viáveis.

A certificação é voluntária. A autoridade de controlo competente ou o Comité Europeu para a Proteção de Dados futuramente vão aprovar critérios para a certificação. O Comité poderá ainda desenvolver critérios para uma certificação comum, o Selo Europeu de Protecção de Dados.

Existem duas vantagens relevantes na certificação:

1. Os Responsáveis e Subcontratantes serão mais facilmente capazes de demonstrar a conformidade, nomeadamente no que respeita à implementação de medidas técnicas e organizacionais.

2. A certificação pode demonstrar que os importadores de dados (Responsáveis, bem como Subcontratantes) localizados fora da UE / EEE implementaram salvaguardas adequadas para os efeitos do artigo 46, i.e., transferências feitas com base num mecanismo de certificação aprovado, em conjunto com compromissos (vinculativos e exigíveis) do importador. Este mecanismo não carece de uma autorização específica por parte de uma autoridade de controlo, afigurando-se, portanto, como uma verdadeira alternativa para a gestão de transferências internacionais.

Reguladores

- Comité Europeu para a Proteção de Dados;
- Autoridades de Controlo Nacionais

Comité Europeu para a Proteção de Dados

O Grupo de Trabalho do Artigo 29, o qual foi estabelecido pela Directiva 95/46/CE ("Directiva de Protecção de Dados") e é atualmente composto por representantes das autoridades de controlo nacionais dos Estados-Membros da UE, juntamente com a Comissão e a Autoridade Europeia para a Proteção de Dados (“AEPD”), será abolido pelo Regulamento. Sendo substituído pelo Comité Europeu para a Proteção de Dados, que será igualmente composto pelos chefes das autoridades de controlo nacionais (ou seus representantes) e da AEPD.

O representante da Comissão no Comité será um membro não-votante e em estados (como a Alemanha) com várias autoridades de controlo, um representante comum deverá ser nomeado nos termos da lei desse Estado-Membro. Em casos de resolução de litígios, em que uma decisão vinculativa deva ser proferida, os poderes de voto da AEPD são restritos às circunstâncias em que os princípios do caso seriam aplicáveis às instituições da UE.

O Comité terá um estatuto reforçado, na medida em que não será apenas comité consultivo, mas um verdadeiro organismo independente da União Europeia com personalidade jurídica própria.

O Comité formalmente representado pelo seu Presidente, que tem o papel principal na organização do trabalho do Comité e, particularmente, na administração do processo de conciliação para disputas entre as autoridades de controlo nacionais. O presidente e dois adjuntos são eleitos de entre os membros do Comité, com mandatos de cinco anos, renováveis apenas uma vez.

As decisões do Comité deverão ser tomadas por maioria simples, mas decisões sobre regras de procedimento e decisões vinculativas (em primeira instância) deverão ser tomadas por uma maioria de dois terços.

Autoridades de Controlo Nacionais

A Autoridades Nacionais de Protecção de Dados (autoridades de controlo) continuarão a existir, tendo como competência central o controlo da aplicação do Regulamento, a proteção dos direitos fundamentais em relação ao tratamento de dados e facilitar a livre circulação de dados pessoais na UE.

As autoridades de controlo têm a obrigação de cooperar entre si e com a Comissão Europeia, a fim de contribuir para a aplicação coerente do Regulamento.

A Comissão deve ser notificada da legislação nacional relativa à criação e nomeação de autoridades de controlo.

As autoridades de controlo devem atuar com absoluta independência (sujeita, contudo, a auditoria financeira e supervisão judicial).

Os Membros das autoridades de controlo devem manter-se independentes, sem influência externa e não devem solicitar ou aceitar instruções de terceiros, nem poderão praticar atos incompatíveis com as suas funções e deveres, nem prosseguir qualquer atividade profissional incompatível, remunerada ou não.

Autoridades de Controlo Nacionais

Competência

As autoridades de controlo serão competentes "para exercer os poderes e desempenhar as funções que lhes são conferidas nos termos do presente regulamento".

O Considerando 122 do Regulamento clarifica, ainda, que esta competência inclui "o tratamento que afete os titulares de dados no seu território, ou o tratamento de dados efetuado por um responsável ou subcontratante não estabelecido na União quando diga respeito a titulares de dados residentes no seu território ".

As autoridades de controlo não têm competência para controlar operações de tratamento efetuadas por tribunais que atuem no exercício da sua função jurisdicional. O termo 'Tribunal' não está definido e não é totalmente clara a extensão da referida regra.

Autoridades de Controlo Nacionais

Atribuições

O artigo 57º do Regulamento compreende uma extensa lista de atribuições das autoridades de controlo nacionais, entre as quais “desempenhar quaisquer tarefas relacionadas com a proteção de dados pessoais ".

As autoridades de controlo devem, portanto, praticar todo e qualquer ato que possa ser razoavelmente interpretado como estando relacionado com a "protecção dos dados pessoais“.

Do conjunto de atribuições, consideramos relevante destacar, o aconselhamento dos governos e parlamentos na elaboração de novas leis, o auxílio dos titulares dos dados, tratamento e investigação de reclamações apresentados por titulares ou entidades representativas, a realização de investigações oficiosas, cooperação com outras autoridades de controlo, acompanhamento das novas técnicas e práticas comerciais no sector das tecnologias de informação.

As autoridades de controlo devem incentivar o desenvolvimento de códigos de conduta e sistemas de certificação, sendo responsáveis pela "elaboração e publicação dos critérios de acreditação" das entidades de certificação e monotorização da aplicação dos referidos códigos de conduta.

Autoridades de Controlo Nacionais

Poderes

O artigo 58º do Regulamento prevê os poderes das autoridades de controlo, os quais poderão ser complementados pelos Estados-Membros, caso assim o desejem. Os poderes atribuídos às autoridades de controlo coincidem, maioritariamente com as atribuições previstas no artigo 57º do Regulamento.

Consideramos relevante, pelo exposto, destacar os elementos não coincidentes de maior importância, como sejam os poderes de: solicitar informações a responsáveis e subcontratantes; realização de auditorias; acesso a instalações e dados; emissão de avisos e advertências e coimas; ordenar o cumprimento do Regulamento e exigir o respeito pelos direitos dos titulares dos dados; proibir o tratamento de dados para fora da UE; aprovação de cláusulas contratuais gerais e regras vinculativas das empresas.

Os Estados-Membros devem conceder às autoridades de controlo os poderes para atuar judicialmente, nomeadamente iniciar (ou participar de outra forma) num processo judicial, com o objetivo de fazer cumprir as disposições do Regulamento. Presumivelmente, a variação existente nos poderes continuará a residir nos termos das leis e procedimentos nacionais.

As autoridades de controlo são obrigadas a apresentar relatórios anuais.

Autoridades de Controlo Nacionais

Cooperação e Consistência

Em casos de tratamento transfronteiriço na União Europeia, a Comissão Europeia propôs um balcão único em que a autoridade de controlo com competência territorial sobre o estabelecimento principal do responsável pelo tratamento de dados, seria a única autoridade competente para fiscalizar e garantir o cumprimento, por parte desse responsável em toda a União Europeia. Em face da forte oposição a proposta da Comissão Europeia foi mitigada.

No termos do Regulamento haverá uma autoridade de controlo principal, nos caso em que o responsável pelo tratamento tenha múltiplos estabelecimentos ou pretenda proceder a um tratamento de dados transfronteiriço na União Europeia. A autoridade de controlo principal será a autoridade com competência territorial no local onde se encontre o estabelecimento principal do responsável pelo tratamento de dados. As autoridades de controlo com competência nos territórios onde se encontrem os demais estabelecimentos (autoridades de controlo interessadas), ou onde residam os titulares dos dados que sejam significativamente afectados, ou junto de quem foi apresentada reclamação, podem ser envolvidas nos procedimentos, obrigando-se a autoridade principal a cooperar.

As autoridades interessadas têm competência para decidir casos puramente locais envolvendo um responsável pelo tratamento transfronteiriço.

Enforcement

Vias de Recurso e Responsabilidade

Os titulares dos dados podem exercer os seguintes direitos (contra Responsáveis pelo Tratamento e Subcontratantes):

- Apresentação de reclamação junto das autoridades de controlo quando os seus dados tenham sido processados de uma forma que não esteja em conformidade com o Regulamento (violação do princípio da legalidade);

- Recurso judicial de decisões proferidas pelas autoridades de controlo ou quando as autoridades de controlo não emitam decisão ou não informem o titular dos dados sobre o estado da reclamação, no prazo de três meses;

- Ação judicial contra Responsáveis pelo Tratamento ou Subcontratantes; e,

- Compensação por danos materiais ou imateriais resultantes da violação do Regulamento.

Os Responsáveis pelo Tratamento ou Subcontratantes têm, também, o direito de recurso aos tribunais nacionais quando seja proferida pela autoridade de controlo competente uma decisão desfavorável juridicamente vinculativa.

O facto de os particulares poderem requerer a compensação por danos morais e não apenas por danos materiais, por certo potenciará as denominadas “class actions”.

Enforcement

Coimas Administrativas

As Autoridades de Controlo beneficiam de poderes para aplicar multas administrativas significativas aos Responsáveis e aos Subcontratantes.

As coimas administrativas podem ser aplicadas pelas Autoridades de Controlo em vez de, ou além de, outras medidas sancionatórias, podendo ser impostas em virtude de um alargado conjunto de infracções, incluindo infracções puramente processuais.

As coimas administrativas são discricionárias e não obrigatórias, podendo impostas numa base casuística e devendo ser "eficazes, proporcionadas e dissuasivas“.

Existem dois níveis de coimas administrativas:

- De menor gravidade, com coimas até € 10.000.000,00, ou, no caso de empresas, até 2% do volume de negócios a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

- De maior gravidade, com coimas até € 20.000.000,00, ou, no caso das empresas, até 4% do volume de negócios a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

Os Estados-Membros podem determinar se, e em que medida, as autoridades públicas podem estar sujeitos a coimas administrativas.

Limitações e Casos Especiais

Os Estados-Membros mantêm a possibilidade de aprovar limitações ao Regulamento quando as mesmas sejam necessárias para fins de segurança nacional, prevenção e detecção de crimes ou situações de interesse público. Em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia, tais limitações devem respeitar "a essência" do direito à protecção de dados e constituírem medidas necessárias e proporcionais.

Para estes fins especiais, o Regulamento requer aos Estados-Membros ou permite aos Estados-Membros a introdução de leis complementares. Nos casos de pesquisa histórica e científica, de tratamento estatístico e de arquivo, poderá ser aprovada uma base legal para o tratamento de dados sensíveis.

Consideramos expectável a aprovação nacional de outros casos especiais, entre os quais se incluem o processamento dos dados dos funcionários, o processamento em conexão com a liberdade de expressão e de sigilo profissional (onde estão previstas restrições de direitos de auditoria pela autoridade de supervisão), ou o processamento de dados religiosos.

Os Responsáveis (e, em alguns casos, os Subcontratantes) terão de verificar e ajustar-se a diferentes abordagens dos Estados-Membros nestas áreas.

Contactos

Rui Pena
rui.pena@cms-rpa.com

José Luís Arnaut
joseluis.arnaut@cms-rpa.com

João Paulo Mioludo
joão.mioludo@cms-rpa.com

João Leitão Figueiredo
joao.figueiredo@cms-rpa.com

Rua Sousa Martins, 10 -1050-218 Lisboa, Portugal
T.: + 351 21 095 81 00 | F.: + 351 21 095 81 55

E.: rpa@cms-rpa.com | W: www.cms-rpa.com

C/M/S/ Law-Now™
Law.Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
www.cms-lawnow.com

C/M/S/ e-guides
Law.Tax

Your expert legal publications online.

In-depth international legal research
and insights that can be personalised.
eguides.cmslegal.com

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices.

CMS locations:
Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Geneva, Glasgow, Hamburg, Istanbul, Kyiv, Leipzig, Lisbon, Ljubljana, London, Luxembourg, Lyon, Madrid, Mexico City, Milan, Moscow, Munich, Muscat, Paris, Podgorica, Prague, Rio de Janeiro, Rome, Sarajevo, Seville, Shanghai, Sofia, Strasbourg, Stuttgart, Tehran, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

www.cmslegal.com