Your World First

C/M/S/ Rui Pena & Arnaut

Meet the Law Newsletter

Propriedade Intelectual

Orientações do Grupo de Trabalho do Artigo 29

Encarregados de Proteção de Dados

Em 16 de Dezembro de 2016, o Grupo de Trabalho sobre Proteção de Dados do Artigo 29 (WP29) publicou algumas das muito antecipadas orientações, juntamente com as Perguntas Frequentes (FAQ), fornecendo mais informações sobre importantes conceitos do Regulamento Geral de Proteção de Dados (Regulamento Geral). Os Interessados têm até o final de Janeiro de 2017 para comentar as orientações entretanto publicadas.

Uma das orientações reporta-se à figura do **Encarregado de Proteção de Dados (EPDs).**

Nos termos do artigo 37. ° do Regulamento Geral de Proteção de Dados, as empresas são obrigadas a nomear um EPD sempre que:

a) O tratamento seja efetuado por uma autoridade ou um organismo público;

b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou,

c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados (por exemplo: saúde, origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, afiliação sindical, dados genéticos, dados biométricos, vida sexual ou orientação sexual) ou dados pessoais relativos a condenações penais e infrações.

Na nova orientação e nas perguntas frequentes, o WP29 discute e esclarece quando deve ser nomeado um EPD e quais os deveres do EPD, realçando-se, desde logo, que o WP29 encoraja todas as organizações a nomearem um EPD.

As orientações do WP29 fornecem aclarações sobre o que se entende por

"autoridade ou organismo público", "atividades principais", "grande escala" e "controlo regular e sistemático" para que as organizações tenham uma melhor perceção sobre as situações em que são obrigadas a nomear um EPD.

i. Autoridade ou Organismo Público

O Regulamento Geral não define o que constitui uma «autoridade ou organismo público», considerando o WP29 que tal conceito deverá ser determinado nos termos do direito nacional. Neste enquadramento, sendo certo que o conceito de "autoridades e organismos públicos" incluirá as autoridades nacionais, regionais e locais, nos termos da legislação nacional de cada Estado-Membro aplicável, poderá incluir múltiplos outros organismos de direito público. Nesses casos, a designação de um EPD será obrigatória.

O WP29 realça o exercício de diversas atividades que, de acordo com a legislação nacional de cada Estado-Membro, poderá ser efetuado não apenas por entidades públicas, mas também por outras entidades reguladas por direito privado ou público, como sejam: serviços de transporte público, abastecimento de água e energia, infraestruturas rodoviárias, serviços públicos de radiodifusão, habitação pública ou organismos disciplinares para profissões regulamentadas.

Nos referidos casos, os titulares dos dados são confrontados com situações muito semelhantes às verificadas quando o tratamento é efetuado por uma autoridade ou organismo público, resultando numa reduzida ou nula possibilidade de escolha por parte dos titulares dos dados. Em virtude das razões expostas, o WP29 considera que a designação de um EPD, quando se verifiquem as referidas condições, pode trazer um elemento de proteção adicional para os titulares dos dados.

ii. Atividades principais:

O considerando 97 do Regulamento Geral esclarece que as "atividades principais" referem-se a "atividades primárias e não se relacionam com o tratamento de dados pessoais como atividades auxiliares". O WP29 adverte que as "atividades principais" podem incluir atividades em que o tratamento de dados constitui uma indestrinçável parte das atividades do responsável pelo tratamento ou subcontratante e identifica o processamento de registros de saúde de um hospital para fornecer cuidados de saúde como exemplo. O WP29 especificamente enfatiza, no entanto, que a folha de pagamentos de uma organização ou atividades de TI são necessárias para apoiar uma empresa e, portanto, são auxiliares e não as atividades principais.

iii. Grande Escala

Embora o considerando 91 do Regulamento Geral ofereça alguma orientação, na verdade, o Regulamento Geral não define o que constitui "grande escala". Nas orientações, o WP29 afirma que a "grande escala" deve ser determinada casuisticamente, tendo em consideração diversos critérios, incluindo o número de pessoas em causa, o volume de dados, a duração, ou a extensão geográfica do tratamento de dados.

Alguns dos exemplos de processamento em grande escala citados são:

i. Tratamento de dados de pacientes no curso regular de negócios por um hospital;

ii. Tratamento de dados de viagem de indivíduos que utilizam o sistema de transporte público de uma cidade;

iii. Tratamento de dados de geolocalização em tempo real de clientes de uma cadeia internacional de fast food para fins estatísticos por um subcontratante

especializado na prestação desses serviços;

iv. Tratamento de dados de clientes no curso regular de negócios por uma companhia de seguros ou um banco;

v. Tratamento de dados pessoais para publicidade comportamental através de um motor de busca; ou,

vi. Processamento de dados (conteúdo, tráfego, localização) por telefone ou provedores de serviços de Internet.

Ao invés, não constituem tratamento de dados em grande escala:

i. Tratamento de dados do paciente por um médico em prática individual; ou,

ii. Tratamento de dados pessoais relativos a condenações e infrações penais por um advogado.

iv. Controlo Regular e Sistemático

O considerando 24 do Regulamento Geral deixa claro que o "controlo do comportamento dos titulares dos dados" inclui o rastreio e a elaboração de perfis na Internet.

Depois de analisar o que se entende por "regular" e "sistemático" nas diretrizes, o WP29 recomenda que o "controlo regular e sistemático" inclua todas as formas de rastreamento e criação de perfis contínuo, recorrente ou periódico, organizado ou sistemático. Alguns dos exemplos listados nas orientações incluem o fornecimento de serviços de telecomunicações; redireccionamento de e-mail; perfis e pontuação para fins de avaliação de risco (por exemplo, pontuação de crédito, prevenção de fraude); publicidade comportamental; controlo de dados sobre bem-estar, aptidão física e saúde através de dispositivos portáteis; dispositivos conectados.

Independentemente de qualquer obrigação legal, o WP29 incentiva as organizações a designar um EPD numa base voluntária. Os requisitos legais do Regulamento Geral serão aplicados, em termos idênticos, aos EPDs voluntários.

Um EPD único, qualificado e autónomo, envolvido em todos os problemas de proteção de dados.

As orientações indicam que uma organização pode designar um único EPD desde que esse indivíduo seja "facilmente acessível a cada estabelecimento". O EPD deve estar em condições de comunicar eficazmente com as pessoas em causa e cooperar com as autoridades de supervisão, o que significa que a comunicação deve ser efetuada no idioma comum dessas partes. O WP29 salienta a importância do EPD estar envolvido em todas as questões relacionadas com a proteção de dados pessoais, os recursos necessários à execução o das funções e a independência do EPD.

O WP29 distingue claramente o papel do responsável pelo tratamento de dados e do subcontratante, os quais são responsáveis pelo cumprimento do Regulamento Geral, e o papel do EDP, que, entre outras coisas, deve auxiliar o responsável ou subcontratante a supervisionar e controlar o cumprimento interno do EPD e tem um dever prestar aconselhamento no que diz respeito à avaliação do impacto sobre a proteção de dados.

As orientações salientam, ainda, a importância de o EPD estar envolvido em todas as questões de proteção de dados na fase mais precoce possível e de os EPD serem dotados dos recursos e do apoio necessários ao cumprimento das

suas funções.

O WP29 define certos requisitos mínimos relativos à experiência e competências de um EPD, que pode ser interno ou externo nomeado, contratado com base num contrato de serviço. As orientações especificamente determinam que a experiência do EPD "deve ser proporcional à sensibilidade, complexidade e quantidade de dados que uma organização processa".

Acresce que, o EPD deve ter um profundo conhecimento do Regulamento Geral e ter experiência em leis nacionais e europeias de proteção de dados e respetivas práticas.

Reconhecendo que o artigo 37.º do Regulamento Geral se aplica tanto aos responsáveis pelo tratamento como aos subcontratantes, o WP29 ressalva a existência de casos não existe a obrigação de designação de um EPD. O WP29 apresenta como exemplos empresas familiares com âmbitos territoriais de atuação bastante limitados ou circunscritos.

Conselhos para as Empresas e Entidades:

- Todas responsáveis pelo tratamento e subcontratantes devem aferir se as regras para designação de um EPD são aplicáveis ao seu caso concreto, devendo documentar a análise interna conduzida na determinação de nomeação ou não de um EPD.
- Os subcontratantes devem fazer uma avaliação independente sobre a necessidade de um EPD, autónoma da realizada pelos responsáveis pelo tratamento de dados.
- As entidades abrangidas pela obrigação de designar um EPD devem: (a) certificar-se de que todos os funcionários compreendam a importância de envolver o EPD em todas as questões de proteção de dados desde o momento inicial da implementação; (b) fornecer ao EPD apoio adequado para que o mesmo possa cumprir as suas funções.
- As entidades não sujeitas à obrigação de designação obrigatória de um EPD devem considerar se desejam designar um EPD numa base voluntária.

Para informação adicional, por favor contacte:

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

João Paulo Mioludo | Advogado Coordenador
joseluis.arnaut@cms-rpa.com

João Leitão Figueiredo
| Advogado Associado
joao.figueiredo@cms-rpa.com

Marrocos e Omã.

CMS Rui Pena & Arnaut is a member of CMS an organisation of independent law firms with 65offices in 38countries around the world.
CMS Presence in europe:
Albania, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, COlombia, Croatia, Cyprus, Czech Republic, France, Germany, Hong-Kong, Hungary, Italy, Luxembourg, Montenegro, Netherlands, Poland, Portugal, Romania, Russia, Scotland, Serbia, Slovakia, Slovenia, Spain, Switzerland, Turkey, Ukraine and United Kingdom
CMS Presence Outside Europe:
Algeria, Brazil, China, Iran, Mexico, Morocco, Oman and United Arab Emirates

www.cms.law