Publicado no Jornal i Online no dia 03/10/2018

OBSERVATÓRIO CONTRA A FRAUDE

Quem proteger? - Dados pessoais ou Criminosos

O regulamento coloca obstáculos significativos ao processo de Due Diligence (DD), introduzindo um novo conjunto de desafios para as empresas que dependem desses dados para os seus programas de prevenção de branqueamento de capitais (AML) e conhecer os seus clientes (KYC).

Nuno Guita (& Gilda Lopes)

"Dados pessoais" é amplamente definido no âmbito do RGPD como "qualquer informação relativa a uma pessoa singular identificada ou identificável". Pode incluir nomes, datas de nascimento, endereços postais e e-mail entre outros. Além disso, o RGPD define o seu tratamento como "qualquer operação ou conjunto de operações que são realizadas em dados pessoais ou em conjuntos de dados pessoais, seja ou não por meios automatizados…" e inclui atividades como "recolha, registo, estruturação, transmissão, etc." dos dados pessoais [(1)].

Por conseguinte, uma instituição financeira que identifique e verifique as informações dos titulares de dados da UE terá de identificar e tratar especificamente as suas obrigações enquanto processador de dados. As obrigações de proteger esses dados estendem-se para fora da UE

Desta forma, alguns dos novos aspetos do RGPD podem sugerir um aparente conflito com as regras de AML em certos países. No coração do desafio de conformidade da RGPD está

O novo "direito ao esquecimento", que permite aos indivíduos solicitarem a exclusão ou remoção dos seus dados pessoais em circunstâncias em que não haja motivo para seu processamento contínuo, bem como "o direito de escolha", que permite que os indivíduos determinem como seus dados podem ser usados, são críticos para o Compliance de protecção de dados pessoais. Porém, para os profissionais de pesquisa e análise e gestão de risco com responsabilidades em diligência prévia (DD) e que necessitam da disponibilidade de dados históricos factuais, isso acarreta um risco, mesmo que a organização tenha concedido ou sobretudo nesses casos.

Encontrar um caminho sustentável para o cumprimento

No confronto paradigmático temos de um lado a protecção de dados e por outro a protecção da reputação tanto da fraude e corrupção como outros crimes. Atento ao Artigo 10 do RGPD, que remete para o artigo 6, para identificar o âmbito da sua própria restrição e que proíbe expressamente o tratamento de dados relativos a antecedentes criminais, excepto se: (1) realizado sob o controlo de uma autoridade oficial europeia ou (2) especificamente autorizada pela legislação da UE ou dos estados membros. No entanto, este articulado baseia-se num entendimento confuso do esquema de proteção de dados de múltiplas camadas.

Ou seja, a menos que uma dessas duas condições seja atendida, investigar o histórico criminal de indivíduos como parte do Due Diligence de suborno pode conflituar com o Regulamento e levar a multas pesadas. Então como verificar atributos de fit and proper para o exercício de administração bancária ou como cumprir requisitos prudenciais anti suborno nos negócios aquando do estabelecimento de parcerias, consórcios internacionais, etc. ??

O objetivo da DD no âmbito por ex. do FCPA ou do UKBA é determinar a existência de indícios de conduta corruptiva de agentes e parceiros comerciais e documentar a prudência preventiva da empresa. Um processo de Due Diligence que desconhece antecedentes criminais dos beneficiários últimos ou que controlam ou agem em nome de terceiros não cumpre a sua função e potencia o envolvimento em condutas impróprias e indesejadas. As empresas têm de aplicar o RGPD aquando do tratamento de todos os dados pessoais, pelo que o estrito cumprimento do Artigo 10, portanto, impediria a investigação do histórico criminal de qualquer pessoa, independentemente de quão corrupto ou suspeita a sua reputação ou a do seu país [(2)].

Who Wins?

Claramente, estamos a assistir a uma mudança no foco para a proteção de dados, particularmente para entidades cujas atividades exige monitoramento em larga escala (Financeiras; Banca, etc….), mas não podemos ignorar que a nova directiva de AML [(3)] exige a todos os seus destinatários, a obtenção de informações adicionais sobre o cliente e o beneficiário efetivo ou os beneficiários efetivos.

Felizmente, existem soluções dentro deste novo ecossistema regulatório que permitem examinar cuidadosamente parceiros, e outras relações comerciais, através do uso inteligente de TI e o cumprimento rigoroso da lei, sem comprometer o RGPD.

Embora essas soluções possam à primeira vista parecer contrárias ao espírito do RGPD, elas são de facto vitais para garantir o cumprimento de leis igualmente importantes, como a Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015 [(4)], relativa à prevenção do branqueamento de capitais ou de financiamento do terrorismo. Como muitas reformas regulatórias abrangentes, também esta traz consigo várias contradições e desafios para as empresas que precisam de conciliar um amplo conjunto de exigências de Compliance.

Eis mais um desafio por vencer e objectivos por conciliar. Até lá andaremos a realizar medidas de diligência prévia no limite da protecção de dados ou da irresponsabilidade prudencial – podemos sempre esperar que a bomba estoire e até enfiar a cabeça na areia.

A chave para o sucesso é aplicar essas mudanças de uma maneira que seja monetariamente sustentável e esteja dentro dos limites das várias estruturas regulatórias nacionais e internacionais.

NOTAS

(1) https://RGPD-info.eu/

(2) http://www.fcpablog.com

(3) DIRETIVA (UE) 2018/843 DO PARLAMENTO EUROPEU E DO CONSELHO de 30 de maio de 2018

(4) https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=celex%3A32015L0849