MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

LEGAL ALERT

REGULAMENTO DORA:

NOVAS NORMAS TÉCNICAS DE REGULAMENTAÇÃO QUANTO À SUBCONTRATAÇÃO DE SERVIÇOS DE TIC

1. Contexto

As Autoridades Europeias de Supervisão (**AES**) publicaram recentemente o Relatório Final relativamente aos Projetos de Normas Técnicas de Regulamentação (*Regulatory Technical Standards* – **RTS**) conforme exigido pelo Artigo 30.º, n.º5 do Regulamento (EU) 2022/2554 relativo à resiliência operacional digital do setor financeiro (**Regulamento DORA**).

Estes RTS estabelecem novos requisitos para as entidades financeiras no que diz respeito à subcontratação de serviços de Tecnologias da Informação e Comunicação (**TIC**), especialmente quanto aos serviços que suportam funções críticas ou importantes, de forma a fortalecer a gestão de risco associado às TIC nestas situações.

De forma alinhada com o Regulamento DORA, os RTS visam reforçar a resiliência digital das entidades financeiras em toda a União Europeia (UE), visando garantir que os riscos associados à subcontratação de serviços de TIC sejam adequadamente geridos e mitigados.

2. Aspetos-chave dos RTS

2.1. Avaliação da subcontratação de TIC

O **Artigo 1.º** dos RTS especifica os elementos que as entidades financeiras devem considerar ao determinar *(i)* a dimensão, *(ii)* o perfil de risco, *(iii)* a natureza, *(iv)* a escala e a *(v)* complexidade dos seus serviços, atividades e operações. Tal inclui a avaliação de fatores como:

- O tipo de serviços de TIC que suportam funções críticas ou importantes ao abrigo do contrato celebrado entre a entidade financeira e o terceiro prestador de serviços de TIC e entre este último e os seus subcontratantes;
- A localização dos subcontratados de TIC e as suas empresas-mãe;
- A extensão e complexidade da cadeia de subcontratação;
- A natureza dos dados partilhados com os subcontratantes de TIC e se os serviços de TIC subcontratados são fornecidos dentro da UE ou em países terceiros, incluindo onde os serviços são prestados e onde os dados são objeto de tratamento e conservação;
- A identificação dos prestadores de serviço TIC intra-grupo e se se encontram registados ou supervisionados por uma autoridade competente de um Estado-Membro da EU ou de um país terceiro;
- A avaliação de concentração de serviços de TIC em um ou poucos subcontratantes;
- A capacidade de trocar de prestadores de serviço de TIC e o risco de disrupção que afetem serviços críticos de TIC ao utilizar subcontratantes.

2.2. Implementação de *standards* uniformes para a subcontratação intra-grupo

O **Artigo 2.º** dos RTS estabelece que a empresa-mãe do grupo da entidade financeira deve garantir que os *standards* se aplicam igualmente aos subcontratantes intra-grupo, o que significa que as entidades dentro do mesmo grupo se encontram sujeitas à mesma supervisão que os terceiros prestadores de serviço, em particular:

- As entidades financeiras devem assegurar que os prestadores de serviços de TIC intra grupo se encontram sujeitos às mesmas avaliações de risco e monitorização contínua que os terceiros prestadores de serviço;
- A empresa-mãe deve implementar práticas de subcontratação consistentes em todas as entidades do grupo, de forma a garantir uma abordagem coesa para a gestão de risco e conformidade.

2.3. *Due diligence* e avaliação de risco para funções críticas

De acordo com o **Artigo 3.º** dos RTS, as entidades financeiras devem aferir, antes de contratar um terceiro prestador de serviços de TIC, se tal prestador de serviços se encontra autorizado ou não a subcontratar total ou parcialmente quaisquer funções críticas, avaliando:

- Se o terceiro prestador de serviços de TIC implementou um processo de *due diligence* para verificar as capacidades operacionais e financeiras potenciais dos seus subcontratantes;
- Se o terceiro prestador de serviços de TIC tem capacidade para identificar e informar a entidade financeira sobre todos os subcontratantes envolvidos e verificar se os contratos com os mesmos permitem que a entidade financeira cumpra as obrigações legais, tais como direitos de acesso para auditorias e inspeções;
- Se o terceiro prestador de serviços de TIC tem recursos, conhecimentos técnicos e estruturas de gestão de riscos adequadas para supervisionar os serviços subcontratados e se a entidade financeira também tem os recursos e estruturas para supervisionar quer o terceiro prestador de serviços TIC como os seus subcontratantes;
- Os riscos relacionados com a localização dos subcontratantes e a concentração de serviços de TIC (incluindo os riscos de uma eventual falha).

Tal avaliação deve ser realizada periodicamente pelas entidades financeiras.

2.4. Condições para a subcontratação de serviços críticos de TIC

De acordo com o **Artigo 4.º** dos RTS, as entidades financeiras devem definir claramente quais os serviços de TIC que suportam funções críticas ou importantes que podem ser subcontratados e sob que condições. Caso seja admissível, os contratos celebrados entre a entidade financeira e o terceiro prestador de serviços TIC devem incluir as disposições contratuais que incidam sobre:

- A responsabilidade do terceiro prestador de serviços TIC pelos serviços subcontratados;
- Requisitos para a monitorizar e disponibilizar relatórios nos serviços subcontratados;
- Avaliação de risco das localizações dos subcontratantes e dos dados partilhados (incluindo a Empresa-Mãe);

- Garantia da continuidade dos serviços e *compliance* com os requisitos de segurança estabelecidos;
- Os direitos de acesso, inspeção e auditoria da entidade financeira quanto aos serviços subcontratados;
- O dever de notificação em casos de alterações materiais aos contratos de subcontratação; e
- Os direitos de rescisão da entidade financeira.

Quaisquer alterações a tais contratos para efeitos de cumprimento do Regulamento DORA devem ser prontamente implementadas e documentadas.

2.5. Requisitos relacionados à cadeia de subcontratação de TIC

O **Artigo 5.**º dos RTS estabelece requisitos para a subcontratação relacionados com a cadeia dos terceiros fornecedores de serviços de TIC, nomeadamente:

- A identificação de toda a cadeia de subcontratantes de TIC envolvidos na prestação de serviços críticos ou importantes, que deve ser atualizada de forma contínua;
- Que a entidade financeira deve manter a responsabilidade geral pelos serviços de TIC prestados por terceiros prestadores de serviços, o que significa que o contrato deverá permitir a monitorização dos riscos de TIC;
- Que o contrato deve incluir disposições que permitam à entidade financeira avaliar o impacto de uma cadeia de subcontratação potencialmente complexa a sua capacidade de monitorizar funções críticas, assim como a capacidade das autoridades competentes supervisionarem a entidade financeira;
- Direitos da entidade financeira de obter informações do terceiro prestador de serviços TIC sobre os contratos de subcontratação e os indicadores de desempenho relevantes.

2.6. Alterações materiais na subcontratação de serviços críticos de TIC

O **Artigo 6.º** dos RTS descreve os procedimentos que as entidades financeiras devem seguir caso surjam alterações materiais aos contratos de subcontratação, que consistem em:

- Implementar um procedimento de notificação de quaisquer alterações materiais nos contratos de subcontratação, no qual o período de pré-aviso deve ser extenso o suficiente

para que a entidade financeira possa avaliar o impacto de tais alterações na sua exposição ao risco e determinar se o terceiro prestador de serviços de TIC ainda consegue cumprir as suas obrigações contratuais;

- O terceiro prestador de serviços de TIC deverá implementar tais alterações propostas às disposições contratuais apenas após a entidade financeira ter aprovado as alterações ou optado por não se opor às mesmas até ao fim do prazo estabelecido;
- Nos casos em que da avaliação de risco da entidade financeira resultar que tais alterações excedem a sua tolerância ao risco, a mesma deverá agir antes do término do prazo, tomando as seguintes medidas:
    - Informar o terceiro prestador de serviços de TIC sobre os resultados obtidos na sua avaliação de risco; e
    - Exercer o seu direito de oposição às alterações e solicitar as modificações que entenda necessárias antes da sua implementação.

2.7. Rescisão do contrato de serviços de TIC

O **Artigo 7.º** dos RTS estabelece as condições em que a entidade financeira tem o direito de rescindir o contrato com o terceiro prestador de serviços de TIC. Tais situações incluem os casos em que terceiro prestador de serviços de TIC:

- Implemente alterações materiais, apesar da objeção da entidade financeira e solicitação de modificações;
- Implemente alterações materiais nos contratos de subcontratação para serviços críticos ou importantes de TIC antes do término do período de notificação e sem a aprovação expressa da entidade financeira; ou
- Subcontrate um serviço de TIC que suporte uma função crítica ou importante que o contrato não permita explicitamente que seja subcontratada.

Próximos passos

Após a adoção dos RTS por parte da Comissão, os mesmos tornar-se-ão obrigatórios e tal exigirá ações por parte das entidades financeiras para garantir conformidade com os mesmos, nomeadamente:

- **Revisão contratual:** avaliar todos os contratos existentes e em vigor com terceiros prestadores de serviços de TIC de forma a garantir que se encontram em conformidade com estes novos requisitos, incluindo as disposições relacionados com a subcontratação e gestão de riscos.
- **Implementação de *frameworks* de gestão de risco:** reforçar os processos internos, incorporando os requisitos de forma a garantir a monitorização contínua dos subcontratantes de serviços de TIC.
- **Comunicação com os subcontrantes:** informar os subcontratantes de serviços de TIC de forma a garantir que entendem os novos requisitos e as responsabilidades associadas ao cumprimento dos mesmos.
- **Auditorias:** preparar-se para eventuais auditorias regulatórias através da revisão e atualização de toda a documentação relevante, particularmente os contratos de serviços de TIC.

Considerações finais

A introdução destes RTS que complementam o Regulamento DORA representa um desenvolvimento importante nos esforços da UE para fortalecer a resiliência operacional digital no setor financeiro.

O Regulamento DORA é aplicável a partir de 17 de janeiro de 2025.

Tanto as entidades financeiras quanto os terceiros prestadores de serviços de TIC devem agir rapidamente para, respetivamente, alinharem as suas práticas de subcontratação e se adaptarem a estes novos requisitos, de forma a evitarem o não cumprimento dos mesmos e reforçarem a sua integridade operacional.

Para maior detalhe sobre como tais alterações podem ter um impacto na sua organização, entre em contacto com a nossa equipa.

Nicole Fortunato
Nuno Sobreira
Ashick Hussein Remetula
Márcia Tomás Pires