JAN. 25

NOTA INFORMATIVA

TECNOLOGIA, MEDIA E TELECOMUNICAÇÕES

Regulamento DORA – *final countdown*: a contratação de terceiros

O Regulamento DORA

A partir de 17 de janeiro de 2025 passa a ser aplicável o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022, *relativo à resiliência operacional digital do setor financeiro* ("**Regulamento DORA**"), *lex speciallis* relativamente à Diretiva (UE) 2022/2555, de 14 de dezembro de 2022, *relativa a medidas destinadas a garantir um elevado nível de cibersegurança na União* – sendo que as entidades abrangidas por esta diretiva continuam sujeitas às obrigações daí resultantes.

Este diploma abrange um amplo leque de instituições financeiras[1] que operem na União Europeia (*e.g.* instituições de crédito, instituições de pagamento, instituições de moeda eletrónica) a par de terceiros prestadores de serviços de TIC[2] (*e.g.* prestadores de serviços de *cloud*) e está em vigor desde 16 de janeiro de 2023, passando agora a ser obrigatório.

O Regulamento DORA visa harmonizar as regras de segurança e resiliência operacional digital no setor financeiro, respondendo à crescente dependência de soluções digitais, que, embora melhorem a eficiência e a inovação, também aumentam a vulnerabilidade a riscos como ciberataques ou falhas técnicas. Para fazer face a estas ameaças, o Regulamento estabelece um regime uniforme de segurança aplicável às instituições financeiras a operar na União Europeia, considerando os efeitos que um único ataque poderia ter no sistema financeiro da União e respetiva estabilidade, em virtude da interligação dos sistemas de informação, e a urgência de prever um quadro comum de combate a estes riscos[3].

O Regulamento harmoniza as regras de segurança e resiliência operacional digital no setor financeiro, respondendo à crescente dependência de soluções digitais.

Pedro Lomba
Marta Salgado Areias
Equipa de Tecnologia, Media e Telecomunicações

1 Artigo 2.º.

2 De acordo com o parágrafo 21) do artigo 3.º, "Serviços de TIC" são "os serviços digitais e de dados prestados por meio de sistemas de TIC a um ou mais utilizadores internos ou externos, de forma contínua incluindo equipamentos informáticos enquanto serviço e serviços de equipamento informático, o que inclui a prestação de apoio técnico através de atualizações de programas informáticos ou microprogramas pelo fornecedor de equipamentos informáticos, com exclusão dos serviços telefónicos analógicos tradicionais".

3 Como assinalado pelo Comité Europeu do Risco Sistémico ("ESRB"), no seu documento sobre "Systemic cyber risk", de fevereiro de 2020, que identificou vulnerabilidades do sistema financeiro associadas à digitalização e riscos cibernéticos.

O Regulamento exige a implementação de mecanismos rigorosos de gestão, incluindo avaliações de terceiros, supervisão contínua e definição de estratégias de saída que garantam a continuidade operacional.

Para tanto, prevê requisitos aplicáveis em matéria de gestão de risco no domínio das TIC, notificação de incidentes, partilha de dados e informações, testes de resiliência operacional digital, medidas de gestão de risco associado às TIC devido a terceiros e cooperação com autoridades, a par de requisitos referentes a acordo contratuais celebrados com prestadores de serviços de TIC, bem como o estabelecimento e execução do quadro de superintendência destes terceiros.

Gestão do risco associado às TIC devido a terceiros

Concretamente no que respeita à contratação de terceiros e gestão de risco associado – um dos pilares do Regulamento DORA – as entidades financeiras devem integrar o risco associado às TIC devido a terceiros no seu quadro de gestão das TIC, aplicando o princípio da proporcionalidade e tendo em conta a natureza, dimensão, complexidade e relevância das dependências criadas pelos serviços em causa. A gestão dos riscos associados a contratos com prestadores de serviços é feita tendo em conta a criticidade ou importância do serviço, processo ou função, a par do impacto potencial na continuidade e disponibilidade das atividades financeiras, tanto individualmente quanto em grupo.

Para mitigar estes riscos, o Regulamento exige a implementação de mecanismos rigorosos de gestão, incluindo avaliações de terceiros, supervisão contínua e definição de estratégias de saída que garantam a continuidade operacional, bem como a previsão de disposições contratuais que devem obrigatoriamente ser incluídas em contratos a celebrar com terceiros prestadores de serviços de TIC.

Disposições contratuais e monitorização contínua

É ainda obrigatório manter um registo atualizado de todos os acordos contratuais relacionados com serviços TIC, assinalando os que envolvem funções críticas ou importantes. O referido registo deve ser disponibilizado às autoridades competentes, sempre que solicitado. Além disso, as instituições financeiras devem comunicar anualmente às autoridades competentes o número de novos acordos, incluindo o número de contratos celebrados, as categorias de terceiros envolvidos, os tipos de acordos e os serviços prestados, bem como as funções abrangidas. A par desta obrigação, as entidades financeiras devem informar as autoridades competentes sobre a intenção de celebrar um contrato relativo a serviços de TIC que apoiem funções críticas ou importantes, bem como, quando uma função passar a ser crítica ou importante.

Antes de celebrar um acordo contratual para a utilização de serviços de TIC, as entidades financeiras avaliam se o serviço apoia funções críticas ou importantes, verificam as condições de supervisão para subcontratação, identificam e avaliam riscos relevantes, incluindo o risco de concentração no domínio das TIC, levam a cabo diligências sobre os potenciais prestadores para garantir a sua adequação e analisam potenciais conflitos de interesse decorrentes do acordo.

PLMJ

Note-se que o risco de concentração em matéria de TIC refere-se à dependência excessiva de um número limitado de prestadores, em virtude da vulnerabilidade das entidades financeiras em caso de falhas, interrupções ou dificuldades desses prestadores, suscetível de comprometer a continuidade e a resiliência das suas operações críticas. Segundo o Regulamento, a avaliação do risco de concentração deve considerar critérios como o número de serviços críticos ou importantes fornecidos pelo mesmo terceiro, o impacto potencial de interrupções nesses serviços e a capacidade de o mercado oferecer alternativas adequadas.

Os contratos devem ser reduzidos a escrito e prever de forma clara os direitos e obrigações de cada uma das partes, prevendo o Regulamento DORA um conteúdo mínimo a incluir nestes contratos, – *i.e.*, devem conter uma descrição clara das funções e serviços a prestar, especificando condições para subcontratação de funções críticas, os locais de prestação dos serviços e tratamento de dados, disposições sobre proteção de dados e recuperação em caso de falha, descrições de níveis de serviço, obrigações de assistência em incidentes, cooperação com autoridades competentes, direitos de rescisão e condições de participação em programas de formação e sensibilização para a resiliência digital. Os acordos contratuais relativos a serviços de TIC que apoiem funções críticas ou importantes devem ainda incluir descrições detalhadas dos níveis de serviço com metas de desempenho rigorosas, períodos e obrigações de notificação de impactos materiais, requisitos para planos de contingência e segurança de TIC, participação em testes de resiliência operacional, direitos de monitorização contínua, incluindo auditorias e inspeções, estratégias de saída com períodos de transição para evitar perturbações, e garantias de migração para outros prestadores ou soluções internas, assegurando a conformidade com os quadros regulatórios.

Responsabilidade e ações necessárias

As instituições financeiras devem identificar todos os fornecedores de serviços de TIC, especialmente os que prestam serviços críticos.

Em suma, o Regulamento DORA estabelece um quadro jurídico atinente à mitigação dos riscos crescentes associados à digitalização do setor financeiro, tendo em vista assegurar maior estabilidade, confiança e resiliência.

As instituições financeiras devem identificar todos os fornecedores de serviços de TIC, especialmente os que prestam serviços críticos, assegurando que os contratos estão em conformidade com o Regulamento DORA. Devem igualmente implementar políticas de *due diligence*, monitorização contínua e auditorias aos fornecedores, levar a cabo análises de risco detalhadas, incluindo riscos de concentração, e estabelecer planos de contingência claros. As instituições devem ainda procurar diversificar os prestadores de serviços de TIC tendo em vista reduzir a exposição a riscos de concentração, garantindo que os contratos incluem mediadas adequadas a garantir a continuidade operacional e estratégias de saída.

A responsabilidade pelo cumprimento deste quadro regulatório recai sobre as instituições financeiras, que enfrentam o desafio de assegurar o cumprimento dos requisitos do Regulamento, mesmo quando lidam com grandes fornecedores e possuem uma capacidade negocial limitada.

Por sua vez, os prestadores de serviços de TIC devem adotar medidas de segurança adequadas, de modo a garantir o cumprimento do regime do Regulamento DORA, estando aptos a negociar a celebração de contratos à luz deste novo regime. ■