CS'Legal Update 01'23

Publicação do Regulamento de Resiliência Operacional Digital (DORA)

André Fernandes Bento
RESPONSÁVEL DE ÁREA
Serviços Financeiros

João Pedro Matias
ESTAGIÁRIO

1. Enquadramento

Em 27 de dezembro de 2022 foram publicados dois Regulamentos da União Europeia relativos à resiliência operacional digital das instituições financeiras, também apelidados de *Digital Operational Resilience Act* ou "**DORA**". [1]

O objetivo do DORA é criar um quadro regulamentar europeu em matéria de resiliência operacional digital, obrigando todas as entidades financeiras a assegurar que são capazes de resistir a todos os tipos de perturbações e ameaças relacionadas com as tecnologias de informação e comunicação (as "**TIC**"), a fim de prevenir e atenuar ciberameaças, perante a generalização da utilização das TIC no setor financeiro.

São desse modo criados requisitos uniformes para a segurança de redes e sistemas de informação de sociedades que operam no setor financeiro e dos terceiros que lhes prestem serviços relacionados com TIC, visando a criação de um quadro regulamentar que dote as entidades financeiras de mecanismos que possibilitem a resistência e resposta a ameaças relacionadas com as TIC.

O DORA será aplicável à generalidade das instituições financeiras, incluindo designadamente instituições de crédito, instituições de pagamento, seguradoras e resseguradoras e empresas de investimento (entre outros), e entrará em vigor a partir de janeiro de 2025, devendo os Estados-Membros da União Europeia adotar legislação que permita a aplicação nacional da mesma até essa data.

Adicionalmente, as entidades que prestem serviços de TIC às instituições financeiras mencionadas também deverão cumprir com o regime previsto no DORA. CS'

[1] Regulamentos (UE) 2022/2554 e a Diretiva (UE) 2022/2556.

2. As principais novidades do DORA

A adoção do DORA implica um conjunto acrescido de obrigações para instituições que se inserem no âmbito de aplicação da mesma, que terão efeitos na *governance* das instituições e em práticas de *compliance* relativas às TIC.

Destacam-se as seguintes novidades introduzidas pelo DORA:

A. Segurança das TIC

O objeto principal do DORA está relacionado com os requisitos de segurança das TIC, estando previsto um conjunto de obrigações que visam assegurar a resiliência das mesmas.

Deste modo, as instituições financeiras ficam obrigadas a estabelecer políticas e protocolos que garantam a segurança e a continuidade dos serviços informáticos, e a monitorizar continuamente essa segurança.

B. *Governance* e gestão de risco

Em matéria de *governance* das instituições vinculadas ao DORA, o novo regime prevê obrigações adicionais relacionadas com as TIC para os órgãos de administração.

Neste âmbito, o órgão de administração das instituições financeiras passa a assumir a obrigação de definir o risco da utilização das TIC na instituição, e de supervisionar esse risco.

No cumprimento deste dever, o órgão de administração deve, nomeadamente:

- Definir políticas internas que visem a manutenção de elevados níveis de disponibilidade, autenticidade, integridade e confidencialidade dos dados;
- Determinar as competências e responsabilidades para todas as funções relacionadas com as TIC, estabelecendo mecanismos adequados de governação para assegurar que essas funções comuniquem, cooperem e se coordenem de forma eficaz e atempada;
- Aprovar uma política de continuidade das atividades no domínio das TIC e fiscalizar a aplicação da mesma;

- Desenvolver um quadro de gestão do risco associado às TIC que inclua, pelo menos, as estratégias, políticas, procedimentos, protocolos e ferramentas de TIC que sejam necessários para proteger devida e adequadamente todos os ativos de informação e de TIC;
- Identificar, classificar e documentar todas as funções operacionais apoiadas pelas TIC, os papéis e as responsabilidades, os ativos de informação e os ativos de TIC que apoiam essas funções, bem como os respetivos papéis e dependências em relação com o risco associado às TIC.

C. Gestão e comunicação de informações sobre incidentes relacionados com as TIC

As entidades financeiras ficam obrigadas a estabelecer um processo de gestão de incidentes relacionados com as TIC que assegure a deteção, gestão e notificação desses incidentes.

O processo de gestão de incidentes deve, designadamente:

- Estabelecer indicadores de alerta precoce;
- Estabelecer procedimentos para identificar, rastrear, registar, categorizar e classificar os incidentes relacionados com as TIC de acordo com a sua prioridade e de acordo com a gravidade e importância dos serviços afetados;
- Atribuir as funções e responsabilidades que devem ser ativadas para os diferentes cenários e tipos de incidentes relacionados com as TIC;
- Estabelecer procedimentos de resposta a incidentes relacionados com as TIC para atenuar os respetivos impactos e assegurar o restabelecimento dos serviços em tempo útil e de forma segura.

Adicionalmente, as instituições financeiras ficam obrigadas a comunicar todos incidentes de carácter severo relacionados com as TIC às autoridades competentes. Esta alteração revela-se como significativa, implicando um escrutínio imediato das instituições competentes perante a ocorrência de um incidente relacionado com as TIC.

D. Testes de resiliência operacional digital

Nos termos do DORA, as instituições financeiras (com exceção das que sejam consideradas microempresas) devem estabelecer um programa de testes de resiliência operacional digital, com o fim de avaliar a preparação para o tratamento de incidentes relacionados com as TIC, identificar pontos fracos, deficiências ou lacunas na resiliência operacional digital e adotar rapidamente medidas corretivas.

E. Terceiros que prestam serviços relacionados com as TIC

O DORA prevê ainda um conjunto de obrigações relativamente à contratação de terceiros que prestem serviços de TIC – sendo que se deve tomar em consideração que, no desenvolvimento do seu quadro de gestão de risco associado às TIC, as entidades financeiras devem considerar o risco associado às TIC como componente integrante do seu próprio risco.

Neste âmbito, é particularmente relevante que as entidades financeiras, antes de contratarem um terceiro para a prestação de serviços de TIC, ficam obrigadas a uma avaliação preliminar do risco de concentração das TIC nesse terceiro, devendo tomar em consideração, designadamente, se estão a celebrar um contrato com um terceiro que não seja facilmente substituível.

Adicionalmente, o DORA prevê um conjunto de matérias que devem ser incluídas nos contratos celebrados com prestadores de serviços de TIC, incluindo:

- A previsão dos acordos de nível de serviço;
- A descrição clara e completa de todas as funções e serviços de TIC a prestar pelo terceiro;
- A previsão de se a subcontratação de funções pelo terceiro é admissível;
- Os locais onde as funções e os serviços de TIC contratados devem ser prestados e onde devem ser tratados os dados;
- A obrigação de o terceiro prestador de serviços de TIC prestar assistência à entidade financeira sem custos adicionais, ou a um custo previamente determinado, caso ocorra um incidente relacionado com as TIC que envolve o serviço de TIC prestado à entidade financeira;
- A obrigação de o terceiro prestador de serviços de TIC cooperar plenamente com as autoridades competentes e as autoridades de resolução da entidade financeira;
- Direitos de rescisão e períodos mínimos de pré-aviso relacionado com a rescisão dos contratos. CS'

3. Os impactos do DORA nas instituições financeiras

O DORA terá impactos significativos para as entidades financeiras, exigindo uma adaptação que vise a implementação de mecanismos relacionados com a resiliência das TIC face ao novo *standard* legislativo imposto.

No contexto português, é expectável que o DORA se revele desproporcionalmente oneroso para as instituições financeiras mais pequenas (por exemplo, IFICs, mediadores, PSPs), em face da sua estrutura de recursos humanos, técnicos e materiais, implicando dificuldades de adaptação.

Por outro lado, representará um quadro regulamentar muito mais exigente do que o atualmente em vigor, aplicável à relação entre as instituições financeiras e os prestadores de serviços de TIC, conduzindo a uma maior exigência na redação dos contratos entre estas entidades, e no trabalho de due diligence da instituições financeiras quanto a estas entidades.

Embora com um prazo de transposição de 2 anos, dada a relevância do DORA e seu importante impacto operacional, é recomendável que as entidades abrangidas iniciem com a brevidade possível um diagnóstico de insuficiências face aos respetivos requisitos, e adotem as alterações ao nível de TIC e de governance com vista a assegurar que os cumprem aquando da data da sua entrada em vigor. CS'