VIEIRA DE ALMEIDA

COMUNICAÇÕES, PROTEÇÃO DE DADOS & TECNOLOGIA

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

VdA EXPERTISE

Janeiro 2023

A evolução tecnológica e os desafios da economia digital têm levado as autoridades europeias a adaptar e harmonizar o quadro regulatório europeu em vários sectores, como o financeiro – um sector cada vez mais digitalizado e, simultaneamente, mais vulnerável a ciberataques e ciber-ameaças.

Neste contexto, foi recentemente publicado o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, relativo à resiliência operacional digital do sector financeiro – o Regulamento de Resiliência Operacional Digital (Digital Operational Resilience Act, doravante "Regulamento DORA" ou "DORA"), disponível aqui.

Este Regulamento, aplicável ao sector financeiro e segurador, faz parte de um pacote legislativo dedicado à resiliência digital, juntamente com a recentemente aprovada Diretiva NIS II[1] e, no que respeita ao sector financeiro, a Diretiva DORA[2].

Ainda que complementares entre si, a Diretiva e o Regulamento DORA têm âmbitos de aplicação diversos: o Regulamento DORA visa estabelecer novos requisitos de segurança dos sistemas e de resiliência operacional digital, com vista a atualizar a abordagem europeia ao risco associado às TIC. Já a Diretiva DORA vem determinar especificamente a alteração de algumas Diretivas europeias[3], garantindo clareza jurídica e coerência com as disposições e requisitos do Regulamento DORA.

A que entidades se aplica o DORA?

O Regulamento DORA é aplicável às entidades financeiras (*e.g.* instituições de crédito, instituições de pagamento, instituições de moeda eletrónica, empresas de investimento, prestadores de serviços de criptoativos, centrais de valores mobiliários, entre outros), às entidades do sector segurador (empresas de seguros e de resseguros; mediadores de seguros, mediadores de resseguros e mediadores de seguros a título acessório), bem como aos prestadores de serviços de TIC (*e.g.* plataformas *cloud*, análise de dados e serviços de auditoria).

Quais os aspetos mais relevantes?

O DORA assenta na responsabilização do órgão da Administração pelos temas de segurança e resiliência, e impõe um conjunto alargado de obrigações, agrupáveis em 5 pilares principais.

Abordamos de seguida algumas das novidades do DORA.

[1] Relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União.
[2] Diretiva 2022/2556 do Parlamento Europeu e do Conselho, de 14 de dezembro. Texto oficial publicado no Jornal Oficial da União Europeia disponível em EUR-Lex - 32022L2556 - EN - EUR-Lex (europa.eu)
[3] Nomeadamente a Diretiva 2009/138/CE, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício, a Diretiva 2013/36/UE, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito, a Diretiva 2014/65/UE, relativa aos mercados de instrumentos financeiros e, ainda, a Diretiva (UE) 2015/2366, relativa aos serviços de pagamento no mercado interno.

Gestão de Risco das TIC

- Implementação e gestão regular de sistemas de governação e quadros de controlo de TIC resilientes, que minimizem o impacto dos riscos associados à sua utilização;
- Documentação e catalogação regular de todas as fontes de riscos das TIC, a fim de se estabelecerem medidas de proteção e prevenção adequadas;
- Implementação de um quadro de risco que permita uma rápida deteção de atividades anómalas, vulnerabilidades e potenciais riscos associados;
- Implementação de uma política de continuidade da atividade das empresas, cópias de segurança e plano de recuperação, assegurando uma rápida e eficaz resposta e recuperação após incidentes;
- Estabelecimento de mecanismos de aprendizagem e evolução dos sistemas de resiliência das TIC, a partir de eventos externos e/ou internos.

Notificações e reporte de incidentes relacionados com TIC

- Implementação de processos de gestão para monitorização e registo de incidentes relacionados com as TIC;
- Classificação de incidentes conforme critérios do DORA e normas técnicas a desenvolver pelas Autoridades Europeias de Supervisão;
- Assegurar a comunicação de incidentes às autoridades competentes, utilizando um modelo comum e um procedimento harmonizado, conforme estabelecido pela respetiva autoridade de supervisão;
- Submeter relatórios iniciais, intermédios e finais sobre incidentes relacionados com as TIC aos utilizadores e clientes da empresa.

Realização de testes de resiliência operacional digital

- Realização periódica de testes de resiliência digital;
- Identificação e eliminação de vulnerabilidades, deficiências ou erros das TIC;
- Criação de requisitos para testes de resiliência operacional digital em termos proporcionais à dimensão das entidades, aos seus respetivos negócios e perfis de risco;
- Conduzir testes de penetração com base em ameaças, para abordar níveis mais elevados de exposição ao risco das TIC.

Partilha de dados e informação

- O Regulamento DORA incentiva a colaboração entre entidades financeiras como elemento essencial para reforçar a resiliência operacional digital, de modo a:
  - Sensibilizar para os riscos das TIC;
  - Minimizar a propagação das ameaças das TIC;
  - Apoiar as técnicas de deteção de vulnerabilidades, estratégias de mitigação ou fases de resposta e recuperação;

- As entidades financeiras são encorajadas a trocar entre si informações sobre ameaças cibernéticas, através de acordos que protejam a natureza potencialmente sensível da informação.

Gestão de risco associado a prestadores de serviços de TIC

- Estabelecer princípios gerais e linhas orientadoras na relação entre entidades financeiras e prestadores de serviços de TIC, através da harmonização de elementos centrais à prestação deste tipo de serviço;
- Assegurar controlo dos riscos e vulnerabilidades decorrentes da dependência de terceiros no domínio das TIC;
- Assegurar que os contratos com prestadores de serviços de TIC disponibilizam toda a informação relativa à monitorização e acessibilidade dos dados (e.g. descrição completa dos serviços a prestar, indicação dos locais onde os serviços são realizados, descrição dos níveis de serviço, disposições sobre acesso, recuperação e devolução de dados, entre outros).

Próximos passos: O que se segue?

O Regulamento DORA entra em vigor 20 dias após a sua publicação no Jornal Oficial da União Europeia.

A partir dessa data, prevê-se um período de implementação de 24 meses para as entidades sujeitas ao novo regime, durante o qual as instituições deverão adaptar os seus sistemas, metodologias e políticas internas ao Regulamento DORA, bem como rever os contratos com prestadores de serviços TICS, para acautelar as disposições contratuais específicas.

Ainda que seja expectável a aprovação de legislação nacional para a execução e desenvolvimento de algumas disposições do DORA, bem como para a transposição da Diretiva, as entidades cobertas deverão desde já iniciar o processo moroso e exigente de implementação do Regulamento DORA.

Como preparar a implementação do DORA?

As entidades cobertas deverão constituir uma equipa multidisciplinar com, pelo menos, elementos dos departamentos jurídicos, *Compliance*, sistemas de informação e cibersegurança.

Numa primeira fase, será essencial identificar os requisitos e efetuar um planeamento exaustivo das várias ações a desencadear, de entre as quais destacamos:

(i) Levantamento dos contratos de prestação de serviços TIC celebrados, com vista a desencadear o processo de revisão e negociação;

(ii) Definição e implementação de políticas e manuais internos de subcontratação e gestão de terceiros (avaliação de prestadores, *due diligence* e auditorias);

(iii) Identificação das vulnerabilidades e riscos associados às TIC, bem como dos mecanismos de resposta a incidentes, ciberataques e ciber-ameaças;

(iv) Definição de modelo de *governance*;

(v) Identificação de políticas e procedimentos a rever/implementar;

(vi) Definição de plano de formação e sensibilização internas.

Contactos

MAGDA COCCO
MPC@VDA.PT

INÊS ANTAS DE BARROS
IAB@VDA.PT

ISABEL ORNELAS
IGO@VDA.PT

MARIA DE LURDES GONÇALVES
MLG@VDA.PT