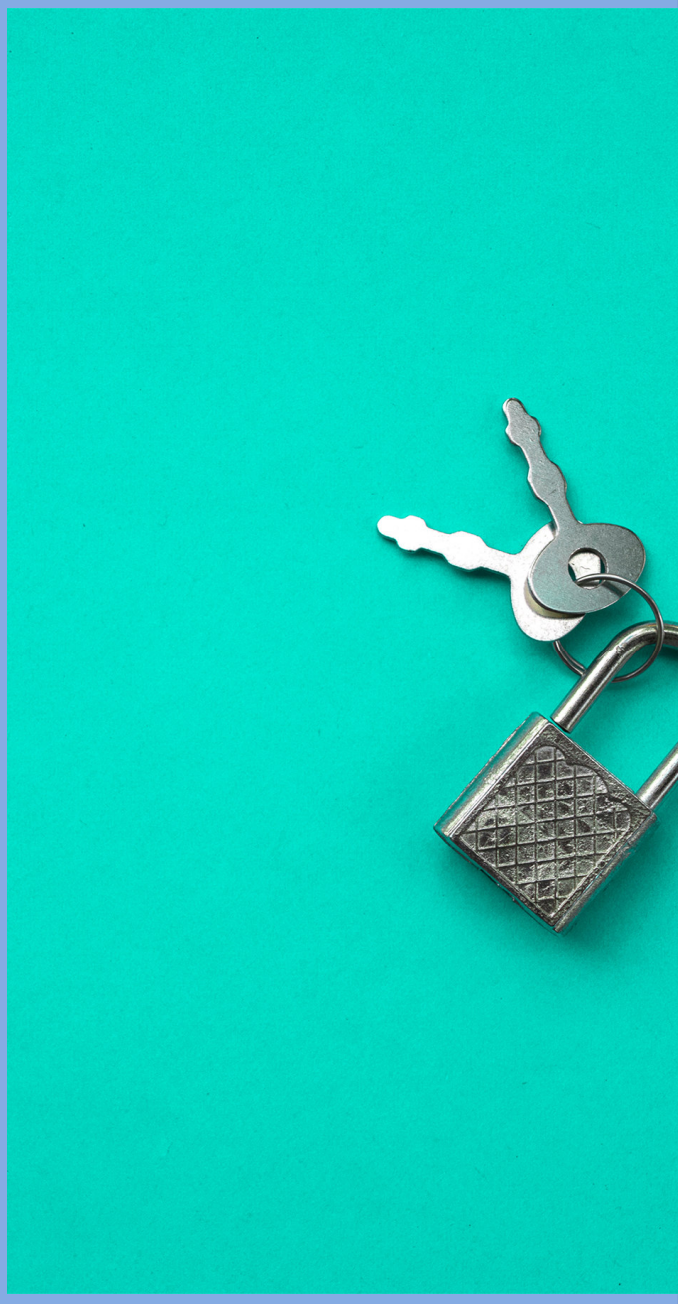
Bird & Bird

NIS 2 Directive, RCE Directive and DORA

Important EU cybersecurity-related legislative acts

January 2023



Important EU cybersecurity-related legislative acts come into force

Three **important EU cybersecurity-related legislative acts** have finally been published in the EU Official Journal on 27 December 2022 and will come into force on **16 January 2023**, these include:

- **Directive (EU) 2022/2555** of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 ("NIS 2 Directive");
- **Directive (EU) 2022/2557** of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC ("RCE Directive"); and
- **Regulation (EU) 2022/2554** of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ("DORA").

All **aiming at strengthening the resilience** of certain entities and partly overlapping in the scope of application, these legislative acts **have different focus areas**. While the NIS 2 Directive aims to respond to the security concerns for the **cyber dimension**, the RCE Directive sets out rules to reduce the vulnerabilities and strengthen **the physical resilience** of critical entities. The DORA on its part, lays down uniform requirements concerning the **security of network and information systems supporting the business processes of financial entities** and addresses both, the **digital as well as physical dimension**. It constitutes the lex specialis regarding the NIS 2 Directive and addresses in a comprehensive manner the physical resilience of financial entities with the consequence that certain provisions set out in the RCE Directive do not apply to those entities.

As to the next steps, by **17 October 2024**, Member States will need to adopt and publish the measures necessary to comply with the NIS 2 as well as the RCE Directive. They will apply those measures from **18 October 2024** and the DORA will apply from **17 January 2025**.

This article describes the key takeaways of the new legislation and highlights some important actions organisations should have in place before the DORA respectively the national implementation of the NIS 2 and RCE Directives apply.

NIS 2 Directive

- **Widening of the scope of the rules:** The NIS 2 Directive, which will replace the NIS Directive, expands the scope to so-called essential and important entities in sectors of high criticality listed in Annex I and other critical sectors listed in Annex II introducing a size-cap rule as a general rule (see the table below).
- **Registration requirements:** The entities falling within scope of the NIS 2 Directive will need to submit certain information to the competent authorities in connection with their registration obligations.
- **Strengthened cybersecurity risk-management requirements:** The entities will need to have certain measures in place (e.g., measures regarding incident handling, business continuity, supply chain security, human resources security, access control policies and asset management) to manage the risks to the security of the network and information systems.
- **More detailed reporting obligations:** The NIS 2 Directive follows a graduated approach with respect to notification of significant incidents to the CSIRT or, where applicable, the competent authority. The entities will also need to notify the recipients of their services in certain cases.
- **Cybersecurity certification:** For the purposes of demonstrating compliance with cybersecurity risk-management measures, Member States may require e essential or important entities to use particular ICT products, services and processes, either developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes.
- **Explicit governance requirements:** The management bodies of essential and important entities will be required to approve and oversee the implementation of the cybersecurity risk-management measures. In addition, the members of these management bodies will be required to follow training and shall encourage entities to offer similar training to their employees on a regular basis.
- **Accountability of top management, supervision and enforcement:** The new legislative act also introduces accountability and liability of top management for the non-compliance with cybersecurity obligations, more stringent supervisory measures for national authorities as well as stricter enforcement requirements and aims to harmonise sanctions regimes across Member States.
- **Administrative fines:** In case of infringements of certain obligations, organisations within the scope of the NIS 2 Directive may be subject to administrative fines [of a maximum of at least 10 000 000 EUR or of a maximum of at least 2% (in the case of essential entities) and of a maximum of at least 7 000 000 EUR or of a maximum of at least 1.4 % (in the case of important entities) of the total worldwide annual turnover in the preceding financial year of the undertaking, to which the respective entity belongs, whichever is higher].

Annex I – Sectors of high criticality	Annex II – Other critical sectors

• Energy
• Transport
• Financial market infrastructure, banking
• Health
• Drinking water, wastewater
• Digital infrastructure
  - Internet Exchange Point providers
  - DNS service providers, excluding operators of root name servers
  - TLD name registries
  - Cloud computing service providers
  - Data centre service providers
  - Content delivery network providers
  - Trust service providers
  - Providers of public electronic communications networks
  - Providers of publicly available electronic communications services
• ICT service management (B2B)
  - Managed service providers (MSP)
  - Managed security service provides
• Public administration
• Space
	• Postal and courier services
	• Waste management
	• Manufacture, production and distribution of chemicals
	• Production, processing and distribution of food
	• Manufacture of medical devices, certain electronic products as well as machinery and transport
	• Digital providers
	  - Providers of online marketplaces
	  - Providers of online search engines
	  - Providers of social networking services platforms
	• Research

RCE Directive

- **Widening of the scope of the rules/critical entities:** The RCE Directive will replace the Directive 2008/114/EC, which was limited to energy and transport sectors, and will cover eleven sectors set out in the Annex (energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space, and production, processing and distribution of food).
- **Identification of critical entities by Member States:** By 17 July 2026, applying certain criteria, each Member State will identify the critical entities for the sectors and subsectors set out in the Annex.
- **Specifics regarding banking, financial market infrastructure and digital infrastructure sectors:** Certain provisions of the RCE Directive will not apply to entities pertaining to these sectors as their resilience is comprehensively covered in the DORA for banking as well as financial market infrastructure and in the NIS 2 Directive for digital infrastructure.
- **Risk assessment:** Critical entities will need to carry out risk assessments within nine months of receiving the notification of their identification as a critical entity, and every four years subsequently in order to assess all relevant risks that could disrupt the provision of their essential services.
- **Technical, security, and organisational measures:** Critical entities will need to take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment.
- **Incident notification:** Critical entities within the scope of the new rules will also need to notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services.
- **Critical entities of particular European significance:** The legislative act also includes certain requirements relating to critical entities of particular European significance, i.e., critical entities providing the same or similar essential services to or in six or more Member States.
- **Supervision and enforcement:** The competent authorities may, following the supervisory actions (on-site inspections, audits) or the assessment of the requested information, order the critical entities concerned to take the necessary and proportionate measures to remedy any identified infringement and to provide the authorities with information on the measures taken.
- **Penalties:** The RCE Directive sets out that Member States will lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to the Directive and take all measures necessary to ensure that they are implemented. The penalties will be effective, proportionate, and dissuasive.

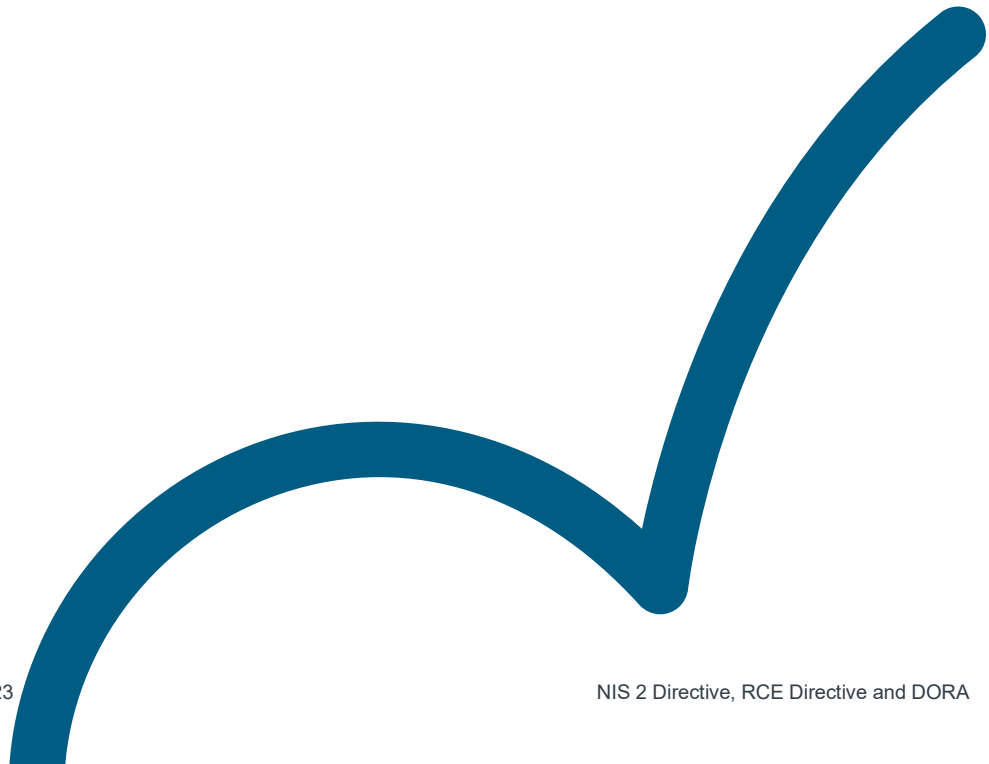
DORA

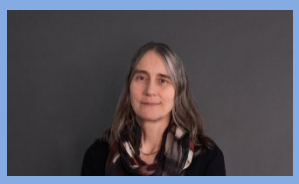
- **Broad scope:** The DORA will apply to a wide range of financial entities (credit institutions, payment institutions, central counterparties, trading venues, insurance and reinsurance undertakings, credit rating agencies, etc.) and information and communication technology (ICT) third-party service providers (including inter alia providers of cloud computing services, software, data analytics services and providers of data centre services).
- **Broad understanding of the term "ICT services":** The term ICT services, used in the context of the DORA is broad, encompassing digital and data services provided through ICT systems, to one or more internal or external users on an ongoing basis (e.g., 'over the top' services, which fall within the category of electronic communications services).
- **Proportionality principle:** As a general principle, when distributing resources and capabilities for the implementation of the ICT risk management framework and complying with certain other obligations under the DORA, financial entities should duly balance their ICT-related needs to their size and overall risk profile, the nature, scale and complexity of their services, activities and operations, while competent authorities should continue to assess and review the approach of such distribution.
- **ICT risk management:** To maintain full control over ICT risk, financial entities will need to have comprehensive capabilities to enable a strong and effective ICT risk management. This includes inter alia implementation of a sound, comprehensive and well-documented ICT risk management framework as part of the financial entities' overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.
- **ICT-related incident management:** Financial entities will also need to have in place specific mechanisms and policies for handling all ICT-related incidents and for reporting major ICT-related incidents.
- **Digital operational resilience testing:** Financial entities should also have policies in place for the testing of ICT systems, controls and processes.
- **Management of ICT third-party risk:** Financial entities will be required to manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with the principles set out in the DORA.
- **Requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities:** The rights and obligations of the financial entity and of the ICT third-party service provider should be clearly allocated, set out in writing and include certain minimum requirements.
- **Critical ICT third-party service provider:** ICT third party service providers designated as critical for financial entities will be subject to particular oversight activities.
- **Administrative penalties and remedial measures:** Competent authorities will have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under the DORA.

What companies should do now

Organisations are advised to act now and assess in particular the following:

- Whether the organisation falls/might fall within the scope of the new legislation;
- What new requirements would need to be implemented by the organisation directly falling within the scope of the new legislation;
- If the organisation is not directly covered by the legislative act(s), whether it deals with suppliers or customers subject to the new rules;
- What obligations do organisations need to attribute to their suppliers in their contractual arrangements to facilitate a seamless, cybersecurity compliant supply chain and to be in conformity with other requirements foreseen by the applicable legislative act;
- Prepare/update processes for incident and threat reporting;
- For suppliers, it will be important to verify whether the Member States in which they operate will mandate the use of certified products, services or processes. Therefore, insight into the regulatory obligations will be also relevant for organisations not directly covered by the new legislative act;
- Assess whether the Commission's implementing acts will result in the harmonisation of additional cybersecurity requirements across the EU;
- Whether there are any related or additional local IT security requirements, which still or would potentially need to be implemented due to any national legislation, and to steer for a coordinated approach in terms of implementation; and
- With respect to the local implementation of the NIS 2 and the RCE Directive, considering the minimum harmonisation approach of both legislative acts, whether EU Member States (intend to) adopt stricter measures.





Marjolein Geus

Partner

+31703538806
marjolein.geus@twobirds.com

Dr. Fabian Niemann

Partner

+4921120056000
fabian.niemann@twobirds.com

Feyo Sickinghe

Of Counsel

+31703538904
feyo.sickinghe@twobirds.com

Dr. Natallia Karniyevich

Associate

+4921120056000
natallia.karniyevich@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw