

NIS2 Directive

2025

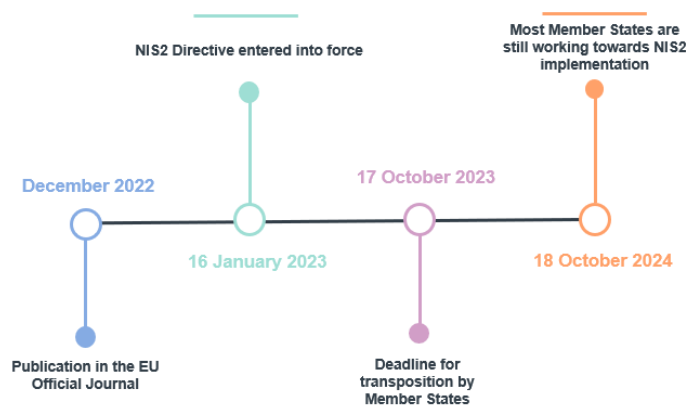
How could the NIS2 Directive be relevant for you?

The NIS2 Directive is gradually replacing the NIS Directive (see our [NIS2 Implementation Tracker](#)). The deadline for transposition by Member States was **18 October 2024**. It applies to **essential** and **important entities** operating in sectors listed in the Directive's annexes where the entities meet certain company size thresholds (see table below). In addition, though not included in the annexes, the NIS2 Directive applies to entities providing **domain name registration services**, **entities identified as critical entities under the CER Directive** (see our [CER Directive Tracker](#)) and, if any Member State so provides, **entities identified before 16 January 2023 as 'operators of essential services'**. There are specific rules in the NIS2 Directive that determine which laws of which Member State may be relevant to the entity, depending, for example, on whether it is a public body, is active in the electronic communications sector, or where it is established in the EU. The NIS2 Directive will directly apply to your organisation if the entity fulfils these criteria and provides the services or carries out the activities within the EU. The NIS2 Directive might be also **indirectly** relevant for you if you deal with customers that are subject to the new rules.

It is not always easy to determine whether the NIS2 Directive applies to an entity, and so we have designed a preliminary assessment tool to check whether your business is likely to be in scope of the new rules. Please **contact your local country** contact if you would like to have us undertake this assessment for you.

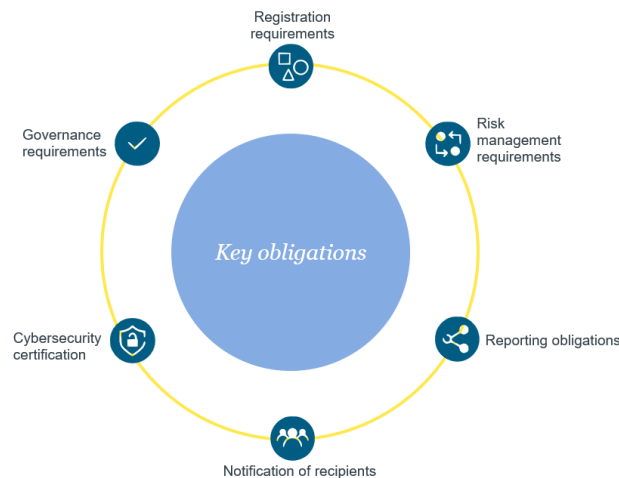
Timeline of NIS2 implementation

The NIS2 Directive entered into force in **January 2023**. By **17 October 2024**, Member States must have adopted and published the measures necessary to comply with this Directive. The majority of Member States is still in a draft phase with their local NIS2 implementations.



What are the key obligations for businesses in scope?

The new NIS2 rules contain specific cybersecurity requirements which in scope entities must comply with, including:



Importantly, the NIS2 Directive follows a **minimum harmonisation approach**: while all Member States must implement new national laws to reflect the NIS2 Directive, the Directive **does not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity**.

As a result, businesses should closely follow the national implementation of the new NIS2 Directive in jurisdictions in which they are regulated, so that appropriate account of the correct set of rules can be considered when implementing new requirements. We have a fixed price monitoring service for those wishing to track developments in one or more EU jurisdictions [here](#).

To find out more, please also check our FAQs and reach out to your local country contact on our cybersecurity webpage [here](#). Our Bird & Bird Connected Newsletter provides further information on the latest developments in cybersecurity (you can subscribe [here](#)).

What are the possible sanctions in case of non-compliance?

Organisations within the scope of the NIS2 Directive that infringe certain provisions may be subject to **administrative fines**.

These levels of possible fines are significant:

- **Essential entities:** a maximum of at least 10 000 000 EUR or of a maximum of at least 2% of the total worldwide annual turnover in the preceding financial year of the undertaking, to which the respective entity belongs, whichever is higher.
- **Important entities:** a maximum of at least 7 000 000 EUR or of a maximum of at least 1.4 % of the total worldwide annual turnover in the preceding financial year of the undertaking, to which the respective entity belongs, whichever is higher.

The laws transposing the NIS2 Directive will also hold senior management personally **accountable and liable** for the non-compliance with cybersecurity obligations, introduce **more stringent supervisory measures** for national authorities as well as providing for **stricter enforcement requirements**.

List of essential and important entities

| Annex I – Sectors of high criticality | | Annex II – Other critical sectors | |
|---|---|---|---|
|  | Financial market infrastructures and banking |  | Waste management |
|  | 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 and providers of publicly available electronic communications services |  | Manufacturing & production Chemicals (also distribution), food (also distribution), medical devices, computer, electronic and optical products, electrical equipment, machinery and equipment n.e.c., motor vehicles, trailers and semi-trailers, other transport equipment |
|  | ICT service management (B2B) Managed service providers and managed security service providers |  | Digital providers Providers of online marketplaces, online search engines and social networking services platforms |
|  | Energy |  | Postal and courier services |
|  | Space |  | Research |
|  | Public administration | | |
|  | Transport | | |
|  | Drinking water and wastewater | | |
|  | Health | | |

Why Bird & Bird?

We advise multinational companies on a range of cybersecurity matters, and almost always in the context of multi-jurisdictional projects.

A snapshot of our recent experience:

- Advising a **global engineering and manufacturing company** with a strong focus on the connected environment on the NIS2 Directive and the Cyber Resilience Act.
- Advising a provider of **high-tech instruments, test equipment and software** on the NIS2 Directive and its applicability to the company's products and services and also advising on the Cyber Resilience Act.
- Advising a **global engineering and manufacturing company** with a strong focus on the connected environment on the NIS2 Directive and the Cyber Resilience Act.
- We advised a **Chinese internet technology company** on the NIS2 Directive in the context of the company's products and services impacted by this legislative act. We have prepared a detailed NIS2 scoping questionnaire and a NIS2 compliance preparation overview allowing the client to prepare for new legislation.
- Advising a **leading supplier of industrial robots and robot software** on NIS2 and other legal/regulatory cybersecurity advice.

How can we support you with compliance?

Bird & Bird's team of experts is on hand to help your organisation prepare for compliance with the incoming rules, including by:

- Carrying out a **scoping exercise** to determine the applicability of the NIS2 Directive to your organisation;
- Tracking and analysis of the **local NIS2 implementation drafts** in the jurisdictions of interest;
- **Reviewing current processes** and procedures to assess what changes need to be made to align with the NIS2 requirements;
- Updating **incident response plans and processes**, including those aimed at compliance with other laws, such as the GDPR;
- Drafting a **practical compliance plan** with specific target dates;
- Assisting with the **procurement of IT capabilities to comply with the NIS2 Directive**, including by drafting relevant contract provisions; and
- **Assisting you** in closing the gap and in ensuring that **regulatory efforts** in related areas (IT contracts, privacy, sector specific laws (e.g. DORA and CER Directive)) are **consistent**.



Contacts



Julie Bak-Larsen

Partner

+4572241212
julie.bak-larsen@twobirds.com



Feyo Sickinghe

Of Counsel

+31703538904
feyo.sickinghe@twobirds.com



Dr. Fabian Niemann

Partner

+4921120056000
fabian.niemann@twobirds.com



Deirdre Kilroy

Partner

+35315749850
deirdre.kilroy@twobirds.com



Berend Van Der Eijk

Partner

+31703538800
berend.vandereijk@twobirds.com



Tomasz Zalewski

Partner

+4825837900
tomasz.zalewski@twobirds.com

twobirds.com

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

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority (SRA) with SRA ID497264. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.