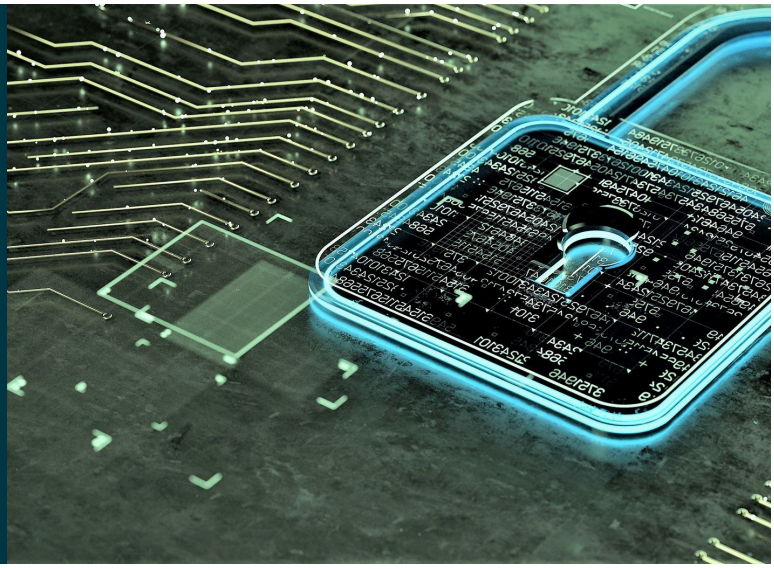
WILSON SONSINI

NIS2: Preparing for EU's New Cybersecurity Rules



CONTRIBUTORS


Laura De Boel


Laura Brodahl


Carol Evrard


Sebastian Andre Thess

ALERTS

April 19, 2024

The European Union (EU) has revised its Cybersecurity Directive (NIS2). The new rules will apply to a wide range of companies in many sectors, create new cybersecurity obligations, and impose high fines for noncompliance. EU countries have until October 17, 2024, to transpose the new rules. As the deadline approaches, companies should assess the impact on their cybersecurity strategy. This alert summarizes the key obligations for businesses.

EU Cybersecurity Framework

In December 2020, the EU Commission published its proposal to repeal the NIS Directive as part of the EU Cybersecurity Strategy. The aim of this strategy is to boost the EU's cyber resilience. Other initiatives include i) new cybersecurity rules for software and hardware products (see the Wilson Sonsini client alert regarding the draft Cyber Resilience Act here); ii) new security requirements in the financial sector (Digital Operational Resilience Act); and iii) new standards for protecting and strengthening critical entities against disruptive incidents (Directive on the resilience of critical entities).

Scope of Application

NIS2 has an extended scope compared to the previous NIS Directive. It applies to "essential" and "important" entities that provide their services or carry out their business activities in the EU. The list of types of entities that are in scope is extensive (see this detailed overview of the scope of NIS2 published by the Belgian Centre for Cybersecurity) and includes:

- companies active in sectors of high criticality such as digital services including cloud services and data center providers, airlines, banks, distribution and transmission system operators, entities carrying out research and development activities of medicinal products, and manufacturers of medical devices that are vital during a public health emergency; and
- companies active in other critical sectors such as social networking platforms, manufacturers of electrical equipment and medical devices, and food production, processing, and distribution companies.

Member States will maintain a list of essential and important entities, subject to a review at least every two years.

Overview of Main New Obligations

The previous NIS Directive required in-scope organizations to take appropriate and proportionate technical and organizational measures to protect their network and information systems from

security threats. It also imposed security incident notification obligations. For more information on the NIS Directive, see the Wilson Sonsini alert here.

NIS2 lists new cybersecurity measures that organizations need to implement, and amends the incident reporting obligations:

- *Cybersecurity Risk Management Requirements.* Companies must implement new cybersecurity risk management measures. Such measures include e.g., i) the adoption of policies (e.g., incident handling policies, policies on risk analysis and information system security); ii) the implementation of cybersecurity training; iii) the adoption of backup management and disaster recovery processes; and iv) the use of encryption and multi-factor authentication, where appropriate. Such measures must be proportionate to the likelihood of an incident occurring, the risk involved, and the severity of an incident's potential impact.
- *Reporting Obligations.* Companies must notify significant incidents to the national "Cyber Security Incident Response Team" (CSIRT) designated by each EU member state. A "significant" incident refers to any cyber-related event that either i) causes, or has potential to cause, severe operational disruption of the service or financial losses for a concerned company; or ii) affects, or has potential to affect, other natural or legal persons by causing considerable material or nonmaterial losses.

Under NIS2, companies must file an early warning within 24 hours after becoming aware of a significant incident and update it through an incident notification within the next 48 hours with further details including an impact assessment. Companies must submit a final incident report to the CSIRT within one month of the submission of the incident notification that should flesh out additional information (e.g., detailed description of the incident, its severity and impact, likely root causes, and mitigation measures).

One-Stop-Shop

Certain essential and important entities (e.g., cloud computing service providers, data center service providers, certain digital providers), established in multiple EU countries will benefit from a one-stop-shop mechanism. Those companies will generally only have to comply with the laws of the country of their main establishment, instead of abiding by the requirements applicable in several jurisdictions. The European Union Agency for Cybersecurity (ENISA) will maintain a confidential registry of these entities.

Sanctions

Companies that infringe reporting or cybersecurity risk management obligations may face the following fines: i) essential entities: up to €10,000,000 or 2.0 percent of their worldwide annual turnover (whichever is greater); and ii) important entities: up to €7,000,000 or 1.4 percent of the worldwide annual turnover (whichever is greater).

Next Steps

EU member states must transpose NIS2 into national law by October 17, 2024, and apply their national laws as of October 18, 2024. Requirements are likely to vary across EU member states, as they may adopt or maintain differing provisions ensuring a higher level of cybersecurity. The UK Government also announced that it will introduce similar obligations in an update to its NIS Regulations.[1] Companies should carefully assess local requirements in their jurisdictions and adapt their cybersecurity strategies as needed.

For more information, please contact Cédric Burton, Laura De Boel, or another member of the firm's privacy and cybersecurity practice.

Laura Brodahl, Carol Evrard, Joanna Jużak, Matthew Nuding, Sebastian Thess, and Hattie Watson contributed to the preparation of this Wilson Sonsini Alert.

---

[1] Cyber laws updated to boost UK's resilience against online attacks, UK Government, Press Release (November 30, 2022): https://www.gov.uk/government/news/cyber-laws-updated-to-boost-uks-resilience-against-online-attacks.