When is a company subject to NIS2 requirements?

Companies will have to perform a self-assessment to determine whether they are subject to the NIS2 Directive. If they are, they will be generally required to register themselves with the Regulated Activities Oversight Authority (RAOA) by 30 June 2024. This article gives practical pointers for the performance of that self-assessment.

I. What is NIS2 exactly?

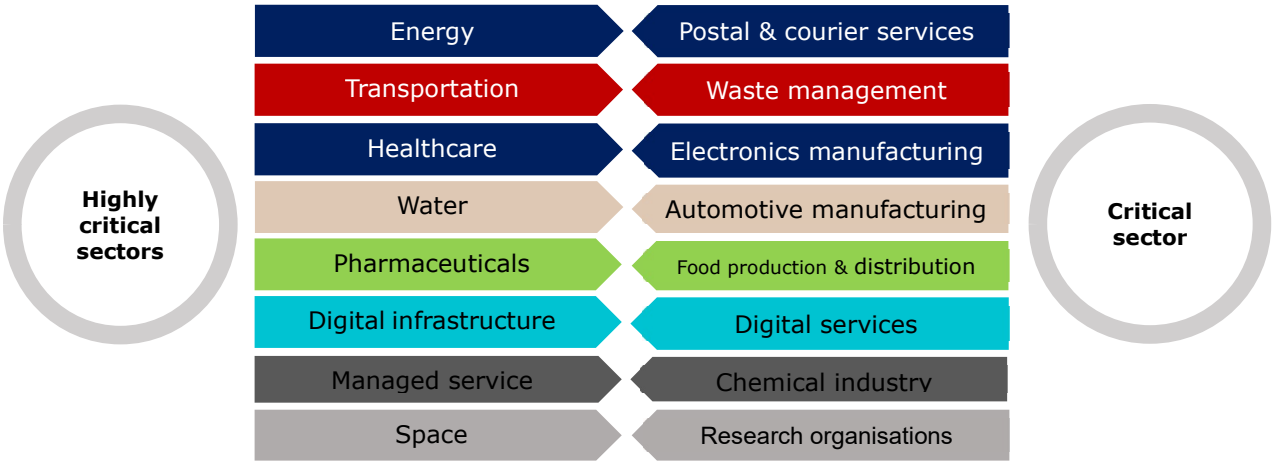
The purpose of NIS2, or Directive (EU) 2022/2555, is to guarantee a high common level of cybersecurity across the European Union through the introduction of various measures that are applicable in all Member States.

The adoption of NIS2 was necessary because network and information systems have become a central feature of everyday life, which has led to an expansion of cyber threats, requiring adapted, coordinated and innovative responses across all Member States, as the differences in legislation introduced by individual Member States can entail additional costs and create difficulties for entities that offer goods or services across borders. This can cause a fragmentation of the internal market and ultimately lead to the higher vulnerability of some Member States to cyber threats, with potential spill-over effects across the European Union.

NIS2 is a directive, and therefore it is not directly applicable; rather, Member States have to transpose it into their own national law. In Hungary, NIS2 compliance is regulated by Act XXIII of 2023 (Cybersecurity Act), but the transposition is not complete at this point and certain details will probably be specified in various implementation decrees.

II. Assessment of activities

The Cybersecurity Act applies to entities that are engaged in the activities listed in Schedules 1 and 2 to the Act. Schedule 1 lists sectors that are classed as 'highly critical', whereas Schedule 2 lists sectors that qualify as 'critical', primarily with the identification of the relevant sectors and subsectors. Certain entities are specifically identified by reference to industry-specific regulations.



[Source: RAOA Cybersecurity Directorate]

III. Size-cap rule – determining the size of an organisation

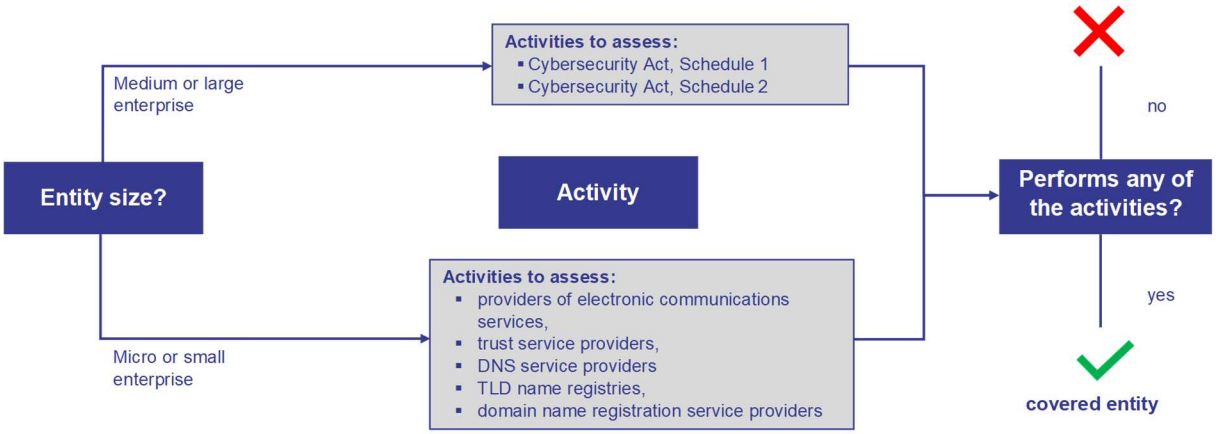
The provisions of the Cybersecurity Act only apply to medium-sized and large enterprises, while micro and small enterprise are not covered by it. Still, there are certain companies in the latter two categories that cannot relax: providers of electronic communications services, trust service providers, DNS service providers, top level domain name registries and domain name registration service providers are in fact covered by the Cybersecurity Act even if they are micro and small enterprises.

The Cybersecurity Act determines whether a company qualifies as a micro or small enterprise with reference to Act XXXIV of 2004 on Small and Medium-Sized Enterprises and on Support for Their Growth, on the basis of the total number of employees and the annual net turnover/balance sheet total. In the case of partner and related companies, however, the figures stated in the Act must be taken into account on a consolidated basis, i.e. on the basis of the consolidated annual report or tax return, or, in the absence of the same, on the basis of the relevant companies' accounts. All this means that a company might not qualify as a medium-sized enterprise in its own right, but it will be treated as such due to owners it shares with other companies.

	micro	small	medium	large	enterprise
number of employees	< 10	< 50	< 250	≥ 250	people
	and	and	and	or	
turnover in previous year	< 2	< 10	< 50	≥ 50	million €
			or	or	
balance sheet total			< 43	≥ 43	million €

[Source: RAOA Cybersecurity Directorate]

Consequently, a company can assess whether it has any obligations under the Cybersecurity Act by determining its size and, if it qualifies on this basis, by looking at whether any of its activities are listed in the Cybersecurity Act or any of its Schedules. This process of assessment is summarised in the table below:



[Source: RAOA Cybersecurity Directorate (adapted)]

The assessment of the figures that determine the size of a company is pretty straightforward, but a more detailed analysis might be required in the case of partner or related companies. The determination of whether a company qualifies as an entity engaged in a particular regulated activity might require a more comprehensive analysis still.

Within the critical sectors listed in Schedule 2 to the Cybersecurity Act, the relevant activities in the manufacturing sector are identified by TEÁOR (i.e. NACE) codes, and therefore companies that have activities that fall under TEÁOR codes 23.5 and 26-30 will qualify as being covered by the Cybersecurity Act.

TEÁOR-based assessment will not work for the rest of the sectors, however, and a simple review of the company extract will not be enough to determine the status of companies in other sectors.

The Cybersecurity Act defines most sectors by reference to other legislation, and therefore if it is questionable whether a particular activity is covered by the Cybersecurity Act, the answer will have to be determined on the basis of a thorough analysis of the relevant legislation. In addition to the legal interpretation of the applicable regulations, it is also advisable to review any permits and licences that may apply to the relevant activity, because these can also help in the assessment of the activity and thereby in the determination of the company's status under the Cybersecurity Act.

***

Authors: András Fenyőházi, Zsanett Szabó és Evelin Varga

If you are interested in more articles on construction law, please visit our website:

Construction Papers

Our mailing address:
CERHA HEMPEL Dezső & Partners
1011 Budapest
Fő utca 14-18
Hungary

E-mail:
andras.fenyohazi@cerhahempel.hu
zsanett.szabo@cerhahempel.hu
evelin.varga@cerhahempel.hu