
3
The most common errors about NIS2 and DORA
www.paytechlaw.com

1

„NIS2 only applies to the IT sector.“

No. NIS2 is aimed at a wide range of sectors that are considered essential to society and the economy. These include not only the IT sector, but also energy, transportation, healthcare, water supply and finance. Organizations in these sectors must therefore comply with the broad security requirements of NIS2, whether or not they are directly involved in the IT sector.

„If you are affected by DORA, you no longer have to pay attention to NIS2."

Wrong. It is true that DORA contains special provisions on IT security for the financial sector and, as a lex specialis, takes precedence over the provisions of NIS2. However, although DORA defines specific requirements for the financial sector, the general requirements of NIS2 must not be ignored as a result. In areas not fully covered by DORA, the NIS2 provisions must therefore still be observed. For example, NIS2 requires cross-sector collaboration and information sharing for all critical infrastructures. DORA does not address this, which is why financial firms must also comply with these NIS2 regulations in addition to the specific requirements of DORA.

„The reporting requirements for IT incidents are identical in NIS2 and DORA.“

No. Both regulations provide for strict deadlines for reporting significant or serious security incidents – such security incidents must be reported within 24 hours of becoming known. Specific reporting formats and reporting channels are available for this purpose, depending on the sector. The very tight reporting deadlines and the basic reporting procedure with initial report (early warning), interim report and final report no later than one month after the initial report are basically identical for NIS2 and DORA. However, DORA, with its corresponding Technical Implementation Standards for reporting, specifies very precise classification requirements for an incident and minimum content for a report, while NIS2 does not provide any precise information in this regard and classifies as reportable any incident that may result in a serious operational disruption or financial loss for the affected organization, or if third parties suffer significant material or immaterial damage as a result of the incident.