
3
Die häufigsten Irrtümer
zu NIS2 und DORA...
www.paytechlaw.com

# 1

## „NIS2 betrifft nur den IT-Sektor.“

**Nein.** NIS2 richtet sich an eine Vielzahl von Sektoren, die als wesentlich für die Gesellschaft und Wirtschaft angesehen werden. Dazu gehören nicht nur der IT-Sektor, sondern auch Energie, Transport, Gesundheitswesen, Wasserversorgung und der Finanzsektor. Unternehmen in diesen Sektoren müssen daher die umfassenden Sicherheitsanforderungen von NIS2 erfüllen, unabhängig davon, ob sie direkt im IT-Sektor tätig sind oder nicht.

# „Wenn man von DORA betroffen ist, muss man NIS2 nicht mehr beachten.“

**Falsch.** Richtig ist, dass DORA spezielle Regelungen zur IT-Sicherheit für den Finanzsektor beinhaltet und als lex specialis Vorrang vor den Regelungen der NIS2 hat. Obwohl DORA spezifische Anforderungen für den Finanzsektor festlegt, dürfen die allgemeinen Anforderungen von NIS2 deshalb aber nicht ignoriert werden. In Bereichen, die DORA nicht vollständig abdeckt, müssen daher dennoch die NIS2-Regelungen beachtet werden. Zum Beispiel verlangt NIS2 für alle kritischen Infrastrukturen eine sektorübergreifende Zusammenarbeit und den Informationsaustausch. DORA trifft hierzu keine Regelungen, weshalb Finanzunternehmen diese NIS2-Regelungen ebenfalls zu beachten und zusätzlich zu den spezifischen Vorgaben von DORA zu erfüllen haben.

# *„Die Meldepflichten bei IT-Vorfällen sind in NIS2 und DORA identisch.“*

Nein. Richtig ist, dass beide Regularien strengere Fristen für die Meldung von erheblichen bzw. schwerwiegenden Sicherheitsvorfällen vorsehen – erhebliche bzw. schwerwiegende Sicherheitsvorfälle müssen innerhalb von 24 Stunden nach Kenntnisnahme gemeldet werden Hierfür stehen spezifische Meldeformate und Meldekanäle je nach Sektor zu Verfügung. Die sehr engen Meldefristen und auch das grundsätzliche Meldeverfahren mit Anfangsmeldung (Frühwarnung), Zwischenbericht und Abschlussbericht spätestens einen Monat nach Erstmeldung sind bei NIS2 und DORA grundsätzlich identisch. Allerdings gibt DORA mit seinen entsprechenden Technischen Regulierungs-/Implementierungsstandards zur Meldung sehr präzise Klassifizierungsvorgaben zu einem Vorfall und Mindestinhalte einer Meldung vor, während NIS2 hierzu keine präzisen Angaben macht und jeden Sicherheitsvorfall als meldepflichtig einstuft, der eine schwerwiegende Betriebsstörung oder finanzielle Verluste für das betroffene Unternehmen nach sich ziehen kann oder wenn Dritte durch den Vorfall erhebliche materielle oder immaterielle Schäden erleiden.