Bundesministerium
Inneres

FMA ÖNB

NISG 2026

DORA als lex specialis zum NISG 2026

BMI IV/S/2
Wien, 2026

§ 24 Abs. 7 Satz 1 NISG 2026

- Für Einrichtungen, die in den Anwendungsbereich von DORA fallen, gehen die einschlägigen Bestimmungen von DORA und nationaler Durchführungsbestimmungen (insb. DORA-VG) vor.
  - „Einschlägige“ Bestimmungen werden nicht näher präzisiert.
  - Verweis auf Art. 1 Abs. 2 DORA welcher festlegt, dass in Bezug auf Finanzunternehmen, die gemäß den nationalen Vorschriften als wesentliche oder wichtige Unternehmen gem. NIS-2-RL ermittelt wurden, **DORA als sektorspezifischer Rechtsakt der Union** gem. NIS-2-RL gilt.

Art. 4 Abs. 1 NIS-2-RL

- Satz 1: Wenn wesentliche oder wichtige Einrichtungen gemäß sektorspezifischen Rechtsakten der Union entweder **Maßnahmen zum Cybersicherheitsrisikomanagement** ergreifen oder **erhebliche Sicherheitsvorfälle melden** müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in der NIS-2-RL festgelegten Verpflichtungen zumindest gleichwertig sind, finden die einschlägigen Bestimmungen der NIS-2-RL, einschließlich der Bestimmungen über Aufsicht und Durchsetzung in Kapitel VII, **keine Anwendung auf solche Einrichtungen**.

- Satz 2: stellt im Gegensatz zu Satz 1 aber auch generell klar, dass, wenn die sektorspezifischen Rechtsakte der Union nicht für alle in den Anwendungsbereich der NIS-2-RL fallenden Einrichtungen eines bestimmten Sektors gelten, die einschlägigen Bestimmungen der NIS-2-RL weiterhin für Einrichtungen zur Anwendung kommen, die nicht unter diese sektorspezifischen Rechtsakte der Union fallen.

§ 27 NISG 2026 bzgl. sektorspezifischer Rechtsakte der EU

- Anforderungen der **§§ 32 (Risikomanagementmaßnahmen)** und **34 (Berichtspflichten)** sind bei bestehenden, zumindest gleichwertigen sektorspezifischen Rechtsakten der EU **nicht anwendbar**.
- Im Zusammenhang mit DORA muss § 27 NISG 2026 aber in Kombination mit oder in Erweiterung durch den vorher angeführten § 24 Abs. 7 Satz 1 NISG 2026 gelesen werden. Eine Einschränkung auf die Nichtanwendung von lediglich §§ 32 und 34 NISG 2026 wäre in richtlinienkonformer Interpretation von Art. 4 NIS-2-RL samt Leitlinien möglw. sogar unionsrechtswidrig.

Schlussfolgerung 1: Welche Bestimmungen des NISG 2026 gelten nicht…

- …für Finanzunternehmen gemäß DORA, welche Kreditinstitute, Handelsplätze oder zentrale Gegenparteien nach der Anlage 1 zum NISG 2026 als wesentliche oder wichtige Einrichtung sind:

Governance (§ 31), Risikomanagementmaßnahmen im Bereich der Cybersicherheit (§ 32), Nachweis der Wirksamkeit von Risikomanagementmaßnahmen (§ 33), Berichtspflichten (§ 34), Vereinbarungen über den Austausch von Informationen zur Cybersicherheit, sofern von der Vereinbarung lediglich Finanzunternehmen umfasst sind (§ 36), Aufsichtsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen (§ 38), Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen (§ 39), damit zusammenhängende Verwaltungsstrafbestimmungen (§ 45)

Schlussfolgerung 2: Welche Bestimmungen des NISG 2026 gelten…

- … für ebendiese (siehe Folie vorher)
- Aus systemischer Sicht bleiben Finanzunternehmen als wesentliche oder wichtige Einrichtungen **Teil des NISG 2026-Regulatoriums**, z.B.
  - im Rahmen der nationalen Cybersicherheitsstrategie (§ 15 NISG 2026),
  - im Rahmen der Aufgabenwahrnehmung durch Computer-Notfallteams (CSIRTs) (§§ 8 ff NISG 2026) oder auch
  - im Rahmen des Managements von Cybersicherheitsvorfällen großen Ausmaßes (§ 16 NISG 2026) und EU-CyCLONe (§ 3 Z 36 NISG 2026).
- Zudem bedarf es auch der **initialen Registrierung** der Finanzunternehmen gemäß § 29 Abs. 2 NISG 2026, da der nationale Gesetzgeber keine explizite Ausnahme von der Pflicht zur Registrierung für Finanzunternehmen vorgesehen hat.

Sonstige Konstellationen: Doppelanwendung

- In sonstigen Konstellationen, in denen Finanzunternehmen dem Anwendungsbereich der DORA unterliegen, aufgrund ihrer konkreten Tätigkeit jedoch zugleich weiteren Sektoren nach Anlage 1 oder 2 zugeordnet werden können, finden DORA und NISG 2026 **grundsätzlich nebeneinander Anwendung**.
- In den Fällen, in denen DORA und das NISG 2026 nebeneinander anwendbar sind, wird es in praxi entsprechend **enge Abstimmung und Zusammenarbeit** zwischen Cybersicherheitsbehörde und DORA Behörde geben, um einen **geregelten und effizienten Vollzug** zu gewährleisten.

Sonstige Konstellationen: Ausnahme Doppelanwendung 1/2

- Eine Doppelanwendung gilt jedoch **nicht**, soweit es sich bei der betreffenden Tätigkeit des Finanzunternehmens gem. DORA um
  - die **Erbringung von IKT-Dienstleistungen** als IKT-Drittdienstleister im Sinne der DORA
  - **gegenüber anderen Finanzunternehmen** handelt.
- In diesen Fällen verbleibt die Tätigkeit im Anwendungsbereich der DORA sowie im Aufsichtsbereich der DORA Behörde.
  → Folglich gehen die einschlägigen Bestimmungen der DORA samt nationalen Durchführungsbestimmungen gemäß § 24 Abs. 7 NISG 2026 auch für diese Tätigkeiten vor.

Sonstige Konstellationen: Ausnahme Doppelanwendung 2/2

- Diese Ausnahme stützt sich sowohl auf die Systematik der DORA sowie Q&A der Europäischen Kommission zur NIS 2 Richtlinie → DORA ist für die Sicherheit von Netzwerk- und Informationssystemen maßgeblich, die die Geschäftsprozesse von Finanzunternehmen unterstützen.

- Demgegenüber soll die NIS 2 Richtlinie nur auf solche Tätigkeiten Anwendung finden, die unter Anhang I oder Anhang II der NIS-2-Richtlinie fallen und nicht bereits vom Anwendungsbereich der DORA erfasst sind.

- Ergänzend stellt die DORA Q&A 136 3193 klar, dass sich der Anwendungsbereich der DORA grundsätzlich auf das gesamte Finanzunternehmen erstreckt und damit auch nicht regulierte Tätigkeiten erfasst, sofern gemeinsame IKT Systeme oder Prozesse genutzt werden und keine vollständige Trennung besteht. **Daraus folgt, dass Finanzunternehmen auch bei der Erbringung von IKT Dienstleistungen grundsätzlich an DORA gebunden sind.**

- Vor diesem Hintergrund erscheint es sachgerecht, auch jene Fälle, in denen ein Finanzunternehmen gegenüber anderen Finanzunternehmen IKT Dienstleistungen im Sinne von Art 3 Z 21 DORA erbringt, der vorrangigen Anwendung der DORA gemäß § 24 Abs. 7 NISG 2026 zu unterstellen, da durch den durchgehenden DORA Anwendungsbereich in dieser Konstellation sichergestellt ist, dass die betreffenden IKT Dienstleistungen **vollständig der Aufsicht durch die FMA unterliegen**.

Sonstige Konstellationen: IKT-Drittdienstleister

- In Art. 2 Abs. 2 DORA wird klargestellt, dass IKT-Drittdienstleister per se nicht zu den Finanzunternehmen zählen.
- Zudem wird gemäß § 24 Abs. 8 NISG 2026 festgelegt, dass kritische IKT-Drittdienstleister per se in den Anwendungsbereich des NISG 2026 fallen.
- Somit gilt für kritische IKT-Dienstleister und IKT-Drittdienstleister, welche die Kriterien für wesentliche oder wichtige Einrichtungen nach dem NISG 2026 erfüllen, **DORA nicht als lex specialis zum NISG 2026, sondern sämtliche Verpflichtungen samt Aufsichtssystem des NISG 2026**.
- Ausnahme hierzu nur bei dem auf den vorherigen Folien (Sonstige Konstellationen: Ausnahme Doppelanwendung) genannten Fall.

Zusammenarbeit/Informationsaustausch zwischen Cybersicherheitsbehörde und DORA Behörde

- Der bidirektionale Austausch von relevanten Informationen und der Zusammenarbeit zwischen der Cybersicherheitsbehörde und DORA Behörde basiert sowohl
  - auf Bestimmungen des NISG 2026 (§ 20) als auch
  - der DORA-Verordnung (Art. 47 Abs. 3 und 4) sowie
  - der aus diesen abgeleiteten und bereits bestehenden Kooperationsvereinbarung.