BKR ZEITSCHRIFT FÜR BANK- UND KAPITALMARKTRECHT

Geschäftsführende Herausgeber: Prof. Dr. Petra Buck-Heeb, Hannover – Prof. Dr. Jens Koch, Köln – Prof. Dr. Philipp Maume, München

Herausgegeben von: Prof. Dr. Markus Artz, Bielefeld – Paul Assies, Rechtsanwalt, Köln – Dr. Heiko Beck, Rechtsanwalt, Frankfurt a. M. – Prof. Dr. Petra Buck-Heeb, Hannnover – Prof. Dr. Jürgen Ellenberger, Vorsitzender Richter am BGH, Karlsruhe – Dr. Markus Escher, Rechtsanwalt, München – Prof. Dr. Dr. Stefan Grundmann, LL.M., Berlin – Dr. Christian Grüneberg, Richter am BGH, Karlsruhe – Prof. Dr. Mathias Habersack, München – Prof. Dr. Ralf Josten, LL.M., Rechtsanwalt, Köln – Dr. Sven Kalisz, Syndikusrechtsanwalt, Berlin – Prof. Dr. Jens Koch, Köln – Dr. Volker Lang, Rechtsanwalt, Bonn – Prof. Dr. Katja Langenbucher, Frankfurt a. M. – Klaus M. Löber, Rechtsanwalt, Frankfurt a. M. – Prof. Dr. Philipp Maume, München – Prof. Dr. Sebastian Omlor, Marburg – Dr. Anika Patz, Berlin – Prof. Dr. Dörte Poelzig, Hamburg – Prof. Dr. Patrick Rösler, Rechtsanwalt, Heidelberg – Prof. Volker Sander, Richter am BGH, Karlsruhe – Prof. Dr. Frank A. Schäfer, LL.M., Rechtsanwalt, Düsseldorf – Dr. Hanno Teuber, Rechtsanwalt, Frankfurt a. M. – Prof. Dr. Stefan Werner, Rechtsanwalt, Frankfurt a. M. – Dr. Kai Zahrte, Ministerialrat, Berlin

Schriftleitung: Prof. Dr. Philipp Maume, München

Redaktion: Arcisstraße 21, 80333 München · bkr.beck.de

22|2025

Seite 1009–1056
25. Jahrgang
19. November 2025

AUFSÄTZE

RENATE PRINZ/DR. NATALLIA KARNIYEVICH*

DORA und NIS2 in der Praxis

Erste Erfahrungen, neue Aufsicht und offene Fragen im Finanzsektor

Die europäische Finanzwirtschaft steht vor einem tiefgreifenden Wandel: Mit der DORA-Verordnung und der NIS2-Richtlinie hat die Europäische Union zwei zentrale Rechtsakte geschaffen, die die digitale Widerstandsfähigkeit von Finanzunternehmen und kritischen Infrastrukturen grundlegend neugestalten. DORA zielt auf die digitale operationale Resilienz des Finanzsektors ab und etabliert erstmals eine direkte Aufsicht über kritische IKT-Dienstleister durch die Europäischen Aufsichtsbehörden. NIS2 erweitert parallel den europäischen Cybersicherheitsrahmen auf 18 Sektoren und schafft sektorübergreifende Mindeststandards. Der Beitrag analysiert die ersten Praxiserfahrungen mit DORA und NIS2, die neuen Aufsichtsstrukturen und die vielfältigen Schnittstellen zu NIS2. Er zeigt, dass beide Regelwerke trotz unterschiedlicher Systematik und Reichweite auf gemeinsamen Grundprinzipien – insbesondere der Einführung der Governance-Vorgaben, einem risikobasierten Ansatz im Umgang mit Cyberbedrohungen, der Verpflichtung zur Meldung von Sicherheitsvorfällen sowie der Stärkung der Sicherheit der Lieferketten – beruhen. Für Finanzunternehmen und ihre IT-Dienstleister bedeutet dies neue Anforderungen, aber auch Chancen: Unternehmen, die frühzeitig integrierte Governance-, Risiko- und Compliance-Strukturen schaffen, können doppelte Pflichten effizienter erfüllen, regulatorische Risiken minimieren und das Vertrauen von Kunden, Aufsicht und Marktpartnern stärken.

I. Einleitung

Die digitale Transformation des Finanzsektors schreitet unaufhaltsam voran – mit ihr wachsen jedoch auch die Risiken. Cyberangriffe, Systemausfälle und Abhängigkeiten von Drittanbietern stellen Finanzunternehmen vor neue Herausforderungen. Die Europäische Union hat mit dem Digital Operational Resilience Act (VO (EU) 2022/2554 – DORA) und der NIS2-Richtlinie (RL (EU) 2022/2555 – NIS2) zwei zentrale Regelwerke geschaffen, um die digitale Widerstandsfähigkeit von Finanzunternehmen und kritischen Infrastrukturen zu stärken.

Die DORA-Verordnung ist Teil des umfassenden Digital Finance Package, das die Europäische Kommission im September 2020 vorgestellt hat. Ziel dieses Maßnahmenpakets ist es, die Wettbewerbsfähigkeit und Innovationskraft des europäischen Finanzsektors zu stärken und gleichzeitig ein hohes Maß an Verbraucherschutz, Marktintegrität und Finanzstabilität sicherzustellen. Das Paket umfasst vier Säulen, die MiCAR-Verordnung, zur Regulierung von Kryptowerten und damit in Zusammenhang stehenden Dienstleistungen, die DORA Verordnung, zur Stärkung der Cyberresilienz, die Überarbeitung bestehender Finanzdienstleistungsrichtlinien, zur Anpassung an digitale Geschäftsmodelle (insb. von MiFID II, Solvency II oder PSD2) sowie verschiedene Maßnahmen zur Förderung grenzüberschreitender digitaler Finanzdienstleistungen, wie zum

*) Die Autorinnen sind Partnerinnen bei McDermott, Will & Schulte Rechtsanwälte Steuerberater LLP.

Beispiel durch den Abbau von Fragmentierung im digitalen Binnenmarkt oder die Förderung digitaler Identitäten.

NIS2 ist flankierend dazu Teil der EU-Digitalstrategie und zielt auf die Cybersicherheit sektorübergreifend in der gesamten Wirtschaft ab. „NIS" steht für „Network and Information Security", die Richtlinie bildet den europäischen Rechtsrahmen zur Erhöhung der Cybersicherheit. Die NIS2-Richtlinie betrifft also nicht speziell den Finanzsektor, sondern insgesamt 18 kritische Sektoren in der gesamten EU, wie Energie, Gesundheit, Verkehr oder Verwaltung und ersetzt die bisherige NIS-Richtlinie aus dem Jahr 2016, deren Anwendungsbereich sie nun deutlich erweitert. Die ursprüngliche RL (EU) 2016/1148 (NIS1) war die erste europaweite Regelung zur Verbesserung der Cybersicherheit. Ihr Ziel war es, ein einheitliches Mindestniveau an Sicherheit für Netz- und Informationssysteme sicherzustellen, insbesondere bei Betreibern wesentlicher Dienste wie Energie, Verkehr, Gesundheit, Wasser und digitalen Infrastrukturen. Die Richtlinie verpflichtete diese Unternehmen dazu, geeignete technische und organisatorische Sicherheitsmaßnahmen zu ergreifen und schwerwiegende Sicherheitsvorfälle zu melden. Zudem mussten die Mitgliedstaaten nationale Cybersicherheitsstrategien entwickeln und sogenannte CSIRTs (Computer-Notfallteams) benennen.

Trotz ihres innovativen Charakters zeigte sich im Laufe der Zeit, dass NIS1 nicht ausreichte, um den wachsenden und komplexer werdenden Cyberbedrohungen zu begegnen. Die Richtlinie war in ihrem Anwendungsbereich zu begrenzt und ließ den Mitgliedstaaten viel Spielraum bei der Umsetzung, was zu uneinheitlichen Sicherheitsniveaus innerhalb der EU führte. NIS2 soll dies nun aufgreifen und den Regulierungsbereich deutlich erweitern, insbesondere erfasst sie auch mittlere und große Unternehmen in weiteren Bereichen. Sie gilt für eine Vielzahl wesentlicher und wichtiger Einrichtungen, darunter auch Finanzunternehmen, sofern und soweit sie nicht bereits vollständig unter DORA fallen.[1]

Während DORA als sektorspezifische Verordnung unmittelbar gilt, bereits seit dem 16. Januar 2023 in Kraft ist und seit dem 17. Januar 2025 vollständige unmittelbare rechtliche Wirkung in allen EU-Mitgliedsstaaten entfaltet, tritt NIS2 als Richtlinie erst durch die entsprechenden nationalen Umsetzungsgesetze in Kraft. Die NIS2-Richtlinie erfolgreich in ihr jeweiliges nationales Recht umgesetzt haben bisher fünfzehn Mitgliedstaaten: *Belgien, Dänemark, Finnland, Griechenland, Italien, Kroatien, Lettland, Litauen, Malta, Rumänien, die Slowakei, Slowenien, Tschechien, Ungarn und Zypern*.[2] Darüber hinaus sind in *Liechtenstein* – als EWR-Staat – am 1. Februar 2025 das neue Cyber-Sicherheitsgesetz und die entsprechende Cyber-Sicherheitsverordnung in Kraft getreten. *Deutschland* beabsichtigt, die nationale Umsetzung bis Ende 2025 bzw. Anfang 2026 abzuschließen.[3]

Die Beziehung zwischen DORA und NIS2 ist dabei klar geregelt: DORA geht als sektorspezifische Verordnung der NIS2-Richtlinie vor, soweit es um Finanzunternehmen geht. Dennoch bestehen zahlreiche inhaltliche Überschneidungen, etwa bei den Anforderungen an das Incident Reporting, das Risikomanagement oder die Governance-Strukturen. Für Unternehmen, die sowohl unter DORA als auch unter NIS2 fallen – etwa bei Mischkonzernen, Unternehmen mit angeschlossenem Zahlungsdienstleister oder gruppenweiten IT-Dienstleistern – ergeben sich daraus praktische Herausforderungen, insbesondere bei der Koordination von Meldepflichten und der Harmonisierung von Sicherheitsmaßnahmen.

Die parallele Existenz von DORA und NIS2 zeigt, dass die EU einen mehrschichtigen Regulierungsansatz verfolgt, um die digitale Resilienz sowohl sektorspezifisch als auch sektorenübergreifend zu stärken. Für die Praxis bedeutet dies jedoch einen erhöhten Abstimmungsbedarf und die Notwendigkeit, regulatorische Schnittstellen frühzeitig zu identifizieren und zu managen.

Ziel dieses Beitrags ist es, die praktische Relevanz und die ersten Erfahrungen mit DORA zu beleuchten, insbesondere auch im Hinblick auf die beginnende direkte Aufsicht über kritische IKT-Dienstleister durch die Europäischen Aufsichtsbehörden („ESAs", bestehend aus der European Banking Authority (EBA), European Securities and Markets Authority (ESMA) und European Insurance and Occupational Pensions Authority (EIOPA)). Zudem wird die Schnittstelle zu NIS2 analysiert, um Überschneidungen, Abgrenzungen und offene Fragen in der Praxis herauszuarbeiten. Der Fokus liegt dabei auf konkreten Herausforderungen, die sich für Finanzunternehmen und deren Dienstleister bereits heute abzeichnen.

II. DORA – Überblick der aktuellen Regulierung und erste Erfahrungen seit Inkrafttreten

DORA verfolgt das Ziel, die Widerstandsfähigkeit von Finanzunternehmen gegenüber den sogenannten IKT-Risiken zu stärken. IKT-Risiken sind dabei alle Risiken, die sich aus der Abhängigkeit von digitalen Technologien und Systemen ergeben und die die Sicherheit, Verfügbarkeit, Integrität oder Vertraulichkeit von Daten und Dienstleistungen beeinträchtigen können. Das ist so umfassend wie schwierig in der Abgrenzung, wie wir im weiteren Beitrag anhand einzelner Praxisfälle zeigen werden.

DORA gilt für alle regulierten Unternehmen des Finanzsektors, dh insbesondere Kreditinstitute, Versicherungsunternehmen, Wertpapierfirmen, Zahlungsdienstleister oder Krypto-Dienstleisters.[4] Digitale Resilienz soll dabei im Finanzsektor eine ähnlich hohe Priorität für die Stabilität im Finanzsektor bekommen, wie die finanzielle Sicherheit, deren Regulierung auf EU-Ebene bereits seit der Finanzkrise massiv verstärkt wurde. Diese Einordnung erscheint richtig. Angesichts der bestehenden Digitalisierung in allen Bereichen des Finanzsektors und der entsprechenden Vernetzung, kann ein Ausfall kritischer Dienstleistungen zu ähnlich hohen Risiken führen wie beispielsweise ein Liquiditäts- oder Eigenmittelengpass, etwa wenn Online-Banking oder Bezahlsysteme ganz oder teilweise nicht mehr verfügbar sind.

1. Kernelemente der DORA-Verordnung

DORA verpflichtet vor diesem Hintergrund Finanzunternehmen dazu, IKT-Risiken systematisch zu identifizieren, zu bewerten, zu überwachen und zu steuern. Dies umfasst Pflichten zur Einrichtung eines IKT-Risikomanagement-Rahmens, die Durchführung von Resilienztests, die Implementierung eines Meldewesens für schwer-

1) Bernau/Lutterbach BKR 2023, 506 (507).
2) Die EU-Mitgliedstaaten sollten die NIS2-Richtlinie bis 17.10.2024 umsetzen – doch viele, darunter auch Deutschland, sind im Verzug. Siehe den NIS2-Umsetzungstracker, https://beck-link.de/28zfh (zuletzt abgerufen am 27.10.2025).
3) Zu der NIS2-Umsetzung in einzelnen Ländern siehe Karniyevich/Emmerich K&R 2025, 366 ff. und K&R 2025, 446 ff.
4) Bernau/Lutterbach BKR 2023, 506 (507).

wiegende IKT-Vorfälle und die Berücksichtigung von IKT-Risiken in der Unternehmensstrategie und Governance. Dabei ist die IT-Sicherheit Teil der ordnungsgemäßen Geschäftsorganisation, zu der schon das KWG verpflichtet. Die BaFin zeigt dabei schon seit einiger Zeit eine hohe Durchsetzungsstärke, wenn sie Mängel in der IT-Organisation von Finanzinstituten feststellt und legt zunehmend auch in Erlaubnisverfahren einen Fokus auf deren Überprüfung.

Die zentralen Regelungsgegenstände von DORA sind wie folgt:

a) IKT-Risikomanagement

Finanzunternehmen müssen ein umfassendes Rahmenwerk zur Identifikation, Bewertung und Steuerung von IKT-Risiken etablieren. Hierdurch soll die Funktionsfähigkeit der Finanzunternehmen insbesondere hinsichtlich Cyber-Gefahren aufrechterhalten oder wiederhergestellt werden.[5] Das Rahmenwerk umfasst u. a. Business Continuity Management, Backup-Strategien und regelmäßige Tests. Eine hervorgehobene Rolle trifft das Leitungsorgan eines Finanzunternehmens, welchem die Letztverantwortung für das Management von IKT-Risiken obliegt. Neben dem regulären IKT-Risikomanagementrahmen sieht die DORA auch ein vereinfachtes Rahmenwerk für kleinere Finanzunternehmen vor.[6]

b) Meldung schwerwiegender IKT-Vorfälle

Es bestehen neue Meldepflichten gegenüber den zuständigen Behörden, die über bestehende Anforderungen (z. B. aus PSD2 oder NIS) hinausgehen. Diese müssen der BaFin über ihre Melde- und Veröffentlichungsplattform (MVP) eingereicht werden. Die Meldung muss so ausgestaltet sein, dass sie der BaFin eine fundierte Einschätzung des Vorfalls, seiner Ursachen, betroffenen Services, Auswirkungen auf Marktteilnehmer, Schwere, Dauer, möglicher böswilliger Herkunft und potenzieller Relevanz für andere Finanzunternehmen ermöglicht.[7]

c) Digitale Prüfungen (Threat-Led Penetration Testing, TLPT)

Größere Institute müssen regelmäßig simulationsbasierte Prüfungen durchführen, um ihre Cyberresilienz zu testen. Hiervon betroffene Unternehmen werden von der BaFin oder im Falle signifikanter Kreditinstitute von der Europäischen Zentralbank (EZB) durch einen Identifikationsbescheid über die Verpflichtung zur Durchführung eines TLPT informiert. Der Testumfang orientiert sich hierbei an dem bereits bestehenden freiwilligen TIBER-EU-Rahmenwerk, sodass die BaFin bei der Anordnung eines TLPT bis dahin durchgeführte TIBER-DE-Tests positiv berücksichtigt.[8] Die EZB hatte im Mai 2018 bereits das sektor-unabhängige Rahmenwerk „TIBER-EU" (Threat Intelligence-based Ethical Red Teaming) veröffentlicht. TIBER-Tests sind spezielle Cyberresilienz-Tests für Unternehmen mit hohem Sicherheitsniveau.[9] Dabei führen externe, ethische Hacker gezielte Angriffe auf kritische Geschäftsprozesse durch, um die Fähigkeit des Unternehmens zur Prävention, Erkennung und Reaktion auf Cyberbedrohungen zu prüfen.[10] Im Gegensatz zu klassischen Penetrationstests beziehen TIBER-Tests auch menschliches Verhalten und organisatorische Schwachstellen in die Szenarien ein. Finanzunternehmen müssen damit aber auch sicherstellen, dass das TLPT auch über Drittdienstleister durchgeführt werden kann und dies entsprechend vertraglich für IKT-Dienstleister und ihre Unterauftragnehmer vereinbaren.[11]

d) IKT-Drittparteienrisiko

Die Anforderungen an das Management von Dienstleistern – insbesondere auch Cloud-Anbietern – wurden erheblich verschärft. Es besteht eine Pflicht zur Führung eines Informationsregisters über alle IKT-Dienstleister, welches bei der zuständigen Aufsichtsbehörde jedes Jahr einzureichen ist.[12] Das Register soll alle vertraglichen Vereinbarungen zwischen Finanzunternehmern und IKT-Drittdienstleistern enthalten. Hiervon erfasst sind auch Unterauftragnehmer, wenn diese kritische oder wichtige Funktionen unterstützen. Die Übermittlung der Informationsregister erfolgt ebenfalls über die MVP der BaFin, wobei bei der Erstellung des Informationsregisters die Vorgaben der ESAs zu beachten sind, an welche die Informationsregister zentral weitergeleitet werden.[13] Auf der Basis dieser Informationen können die ESAs dann bestimmen, welche IKT-Dienstleister sogenannte kritische IKT-Dienstleister sind, über die eine direkte Aufsicht eingeführt wird.

e) Aufsicht über kritische IKT-Dienstleister

Die ESAs erhalten erstmals direkte Aufsichtsrechte gegenüber bestimmten Drittanbietern, dh über IKT-Dienstleister, die selbst keine Finanzunternehmen sind und die grundsätzlich bisher nur mittelbar der Finanzmarktregulierung unterlagen. Die Aufsicht soll ausdrücklich nicht der eigentlichen Finanzmarktaufsicht gleichgesetzt werden, sondern mehr eine Art Überwachung darstellen (im englischen "Oversight" vs. "Supervision")[14]. Eine federführende Überwachungsbehörde aus dem Kreis der ESAs, die sich nach der schwerpunktmäßigen Branche eines IKT-Drittdienstleisters richtet, erhält hierzu Informations-,Kontroll- und Prüfrechte (siehe Abschnitt III).[15] Viele IKT-Dienstleister, die erste Anfragen der ESA erhalten haben, stellt dies für große Herausforderungen, was den Umgang mit der neuen Aufsicht und die interne Organisation angeht. Die Mechanismen und das Knowhow, die direkten Anfragen der Aufsichtsbehörden zu handeln und einordnen zu können, fehlt naturgemäß weit überwiegend, ebenso fehlt den ESAs oftmals ein guter Überblick über den Aufbau und die Dienstleistungen, die die IKT-Dienstleister ausführen, um ihre Aufsicht richtig aufzubauen und einsetzen zu können.

2. Erste Erfahrungen aus der Praxis

In der Praxis zeigen sich bereits erste Herausforderungen bei der Umsetzung:

Besonders aufwendig stellte sich bereits zu Jahresbeginn die Erstellung und Pflege des *Informationsregisters* heraus, welches

5) Bernau/Lutterbach BKR 2023, 506 (509).
6) BaFin, IKT-Risikomanagement, v. 28.8.2025, https://beck-link.de/7844v (zuletzt abgerufen am 27.10.2025).
7) BaFin, Meldung schwerwiegender IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen, v. 20.1.2025, https://beck-link.de/6c8a5 (zuletzt abgerufen am 27.10.2025).
8) BaFin, Testen der digitalen operationalen Resilienz einschließlich TLPT, https://beck-link.de/5rk4s (zuletzt abgerufen am 27.10.2025).
9) BaFin, BaFin Perspektiven 1 | 2020 v. 25. Mai 2020, https://beck-link.de/m3h52 (zuletzt abgerufen am 27.10.2025).
10) Vgl. Bernau/Lutterbach BKR 2023, 506 (511).
11) Vgl. Lauck BKR 2025, 124 (132).
12) Bernau/Lutterbach BKR 2023, 506 (511).
13) Entsprechende Formulare und Verweise auf die Vorgaben der ESAs finden sich unter https://beck-link.de/htz3n (zuletzt abgerufen am 27.10.2025).
14) EIOPA: Informationen zum DORA Oversight, https://beck-link.de/w54mv (zuletzt abgerufen am 27.10.2025).
15) BaFin, Überwachungsrahmen für kritische IKT-Drittdienstleister, https://beck-link.de/f5pky (zuletzt abgerufen am 27.10.2025); Bernau/Lutterbach BKR 2023, 506 (513); Schmidt WM 2024, 2125 (2133 f.).

sämtliche IKT-Dienstleister und deren Leistungen strukturiert erassen muss. Je nach Institutsgröße ergaben sich Listen von wenigen einzelnen IKT-Dienstleistern bis hin zu Listen mit IKT-Dienstleistern in hoher zweistelliger Anzahl. Die Einordnung als IKT-Dienstleister warf dabei in der Praxis einige zunächst ungeklärte Fragen auf. Ab wann ist ein Dienstleister eines Finanzunternehmens ein IKT-Dienstleister? Reicht dafür beispielsweise schon die regelmäßige digitale Übermittlung von Daten zu einzelnen Assets, an denen das Institut beteiligt ist? Wenn die Übermittlung der Daten über eine digitale Schnittstelle erfolgt, lässt sich das unter DORA argumentieren, scheint aber gleichwohl nicht folgerichtig, da dies keine Relevanz für die digitale Resilienz des Instituts haben dürfte. Für den Dienstleister, der die Daten übermittelt, hat die Anwendbarkeit von DORA aber durchaus erhebliche Auswirkungen, da diesen dann auch die entsprechend hohen Sicherheitsstandards treffen und Verträge an andere Standards anzupassen sind, was das alltägliche Handling insgesamt erschwert. Hier waren in der Praxis viele verschiedene Ansätze der Umsetzung zu sehen, ob Institute zu einer breiten oder eher engen Auslegung der Definition ihrer IKT-Dienstleister neigten. Ebenso geht es dann weiter, wenn es bei den IKT-Dienstleistern selbst um die Definition ihrer Unterauftragnehmer geht. Die im Juli erschienenen technischen Regulierungsstandards (RTS) der EU-Kommission (Delegierte VO (EU) 2025/532, am 24. März 2025 veröffentlicht, seit dem 22. Juli 2025 verbindlich) verhalten sich zwar auch zur Definition und Behandlung von IKT-Dienstleistern und deren Unterauftragnehmern im Rahmen von DORA und konkretisieren hier die Regulierung, lassen aber auch weiterhin viel Interpretationsspielraum für die einzelnen Praxisfälle offen. Für viele Einzelfälle wird man wohl die Verwaltungspraxis und bestenfalls ausdrückliche Klarstellungen abwarten müssen.

Auch die *Vertragsprüfung* stellt viele Institute vor Schwierigkeiten. Bestehende Vereinbarungen genügen oftmals noch nicht den Anforderungen aus Art. 28 ff. DORA, gleichwohl wir in Deutschland durch die bereits bestehende Regulierung über die MaRisk und die BAIT/ZAIT/VAIT/KAIT bereits von einem vergleichsweise hohen Standard gestartet sind.[16] Die Anpassungsprozesse gestalten sich in der Praxis vielfach langwierig und mitunter herausfordernd, insbesondere wenn es darum geht, großen internationalen IKT-Dienstleistern, zu denen oftmals auch inländische Alternativen fehlen, die eigenen DORA relevanten Vertragsstandards aufzwingen zu müssen.[17]

IKT-Dienstleister müssen sich auf ein *strukturiertes Management ihrer Beziehungen* über den gesamten Lebenszyklus einstellen, von der *Auswahl der IKT-Dienstleister* selbst, der Einbringung ihrer *Unterauftragnehmer*, über die Vertragsgestaltung, das *laufende Monitoring* bis hin zum *Exit-Management*. Die Prozesse über eine Einigung gestalteten sich hier mitunter langwierig, auch angesichts divergierender Interpretationen der Verordnung. Gerade für kleinere nationale IKT-Dienstleister dürfte sich oftmals die Frage stellen, ob sich die Erbringung der Dienstleistungen im Finanzsektor bei dem hohen Maß an Regulierung finanziell noch lohnt.[18] Die vollständige Anpassung der Vertragswerke ist vielfach bis heute noch nicht vollständig abgeschlossen. Es steht zu erwarten, dass gerade bei den großen IKT-Dienstleistern die direkte Aufsicht durch die ESAs noch entsprechenden Einfluss auch auf die Vertragsgestaltung bringen wird.

Zudem erfordert die Umsetzung ein *hohes Maß an Governance*, etwa durch die klare Zuweisung von Verantwortlichkeiten, die Einbindung der Geschäftsleitung und die Integration von IKT-Risiken in das unternehmensweite Risikomanagement. In Deutschland besteht hier bereits durch die schon vor DORA bestehende Regulierung ein hohes Maß an IT-Risiko und Governance Strukturen. Vielfach mussten jedoch gerade für das Vertrags- und Informationsregistermanagement nochmal Kapazitäten geschaffen werden.

Die Liste an ersten Implementierungsschwierigkeiten könnte wohl noch mit vielen Beispielen fortgeschrieben werden, wie beispielsweise auch Einzelfragen bei der Nutzung interner IKT-Dienstleister und genaue Anforderungen an die Überwachung von IKT-Dienstleistern durch die Finanzunternehmen selbst.

Diese ersten Erfahrungen zeigen, dass DORA nicht nur technische, sondern auch organisatorische und strategische Anpassungen erfordert – und damit weit über die reine IT-Implementierung hinausgeht.

III. Die neue Aufsicht über kritische IKT-Dienstleister durch die ESAs

Wie schon dargestellt, ist ein zentrales Novum der DORA-Verordnung die Einführung einer direkten Aufsicht („*Oversight*") über bestimmte IKT-Dienstleister durch die Europäischen Aufsichtsbehörden, ESAs. Diese Oversight betrifft Dienstleister, die als „kritisch" für die Stabilität und Sicherheit des Finanzsystems insgesamt eingestuft werden, weil ihr Ausfall bspw. eine Vielzahl von Finanzunternehmen in der EU betreffen würde.[19]

1. Kriterien für die Einstufung als „kritischer IKT-Drittdienstleister"

Die Einstufung erfolgt durch die ESAs auf Basis mehrerer Kriterien, darunter:

- Anzahl und Bedeutung der Finanzunternehmen, die den Dienstleister nutzen;
- Art der erbrachten Dienstleistungen (zB Cloud-Infrastruktur, Datenanalyse, Zahlungsverarbeitung);
- Systemische Risiken, die aus einem Ausfall oder einer Störung resultieren könnten;
- Grad der Substituierbarkeit des IKT-Drittdienstleisters.

Die Einstufung erfolgt auf der Grundlage der Informationsregister, welche die zuständigen nationalen Behörden an die ESAs weitergeleitet haben.[20] Nach jetzigem Stand ist eine finale Einstufung der Drittdienstleister als kritische IKT-Drittdienstleister und der Beginn der Beaufsichtigung dieser für das Ende dieses Jahres geplant.[21] Die avisierten kritischen Dienstleister wurden aber bereits von den ESAs kontaktiert und um Stellungnahmen zu ihrer Einordnung gebeten.

Die ESAs werden zukünftig jährlich eine Liste der kritischen Dienstleister veröffentlichen. Diese Einstufung hat weitreichende

16) Vgl. Merwald RDi 2024, 590 (592).
17) Hierzu Schäfers VersR 2025, 1225 ff.
18) Vgl. Schäfers VersR 2025, 1225 (1234).
19) Vgl. Art. 31(2) lit. a DORA sowie Delegierte Verordnung C(2024) 896 final.
20) Vgl. EBA, Pressemitteilung v. 18.2.2025, https://beck-link.de/543pf (zuletzt abgerufen am 27.10.2025).
21) Vgl. EBA, Pressemitteilung v. 18.2.2025, https://beck-link.de/543pf (zuletzt abgerufen am 27.10.2025).

Folgen für die betroffenen Unternehmen. So hat die federführende Überwachungsbehörde der ESAs weitreichende Informations-, Kontroll- und Prüfrechte, welche zwangsgeldbewährt sind. Sollte diese etwa erhebliche Missstände beim IKT-Risikomanagement des Drittdienstleisters feststellen, kann sie an diesen Empfehlungen aussprechen oder die nationalen Überwachungsbehörden können die Finanzunternehmen dazu auffordern, die Zusammenarbeit mit dem Drittdienstleister zu unterbrechen oder sogar zu beenden. Zur Finanzierung des Überwachungsrahmenwerks werden von den kritischen IKT-Dienstleistern Überwachungsgebühren erhoben.[22]

2. Aufsichtsmechanismen der ESAs

Die ESAs erhalten umfassende Befugnisse zur Durchführung von Prüfungen und zur Überwachung der kritischen Dienstleister. Dazu gehören:

- Joint Examination Teams (JETs): Interdisziplinäre Teams aus den drei ESAs führen koordinierte Prüfungen durch.
- Zugriffsrechte: Die ESAs können Informationen, Dokumente und Daten direkt vom Dienstleister anfordern.
- Empfehlungen und Maßnahmen: Bei festgestellten Mängeln können die ESAs Empfehlungen aussprechen oder – in schwerwiegenden Fällen – Maßnahmen wie die Einschränkung bestimmter Dienstleistungen verlangen.
- Die betroffenen Dienstleister müssen zudem einen Oversight-Plan vorlegen, der ua Risikomanagement, Incident Response und Business Continuity umfasst. Die ESAs prüfen diesen Plan regelmäßig und können Anpassungen verlangen.

3. Auswirkungen auf Finanzunternehmen

Für Finanzunternehmen bedeutet die neue Aufsicht, dass sie bei der Auswahl und Steuerung von Dienstleistern künftig auch die potenzielle Einstufung als „kritisch" berücksichtigen müssen. Verträge mit solchen Dienstleistern müssen besondere Anforderungen erfüllen, etwa hinsichtlich Audit-Rechten, Exit-Strategien und Datenzugriff.[23] Zudem sind Institute verpflichtet, die Zusammenarbeit mit kritischen Dienstleistern in ihrem Informationsregister besonders zu kennzeichnen.

In der Praxis ist zwischen der Einstufung eines IKT-Dienstleisters als „kritisch" durch ein Finanzinstitut und der Einstufung als „kritischer IKT-Dienstleister" im Sinne der DORA-Oversight durch die ESAs zu unterscheiden. Ein Dienstleister kann für ein einzelnes Institut kritisch sein, ohne dass er für den gesamten Finanzsektor systemische Relevanz besitzt. Diese Differenzierung führt häufig zu Unsicherheiten, insbesondere hinsichtlich der Pflichten der Institute gegenüber Dienstleistern, die unter ESA-Aufsicht stehen. Zwar besteht keine Verpflichtung, bevorzugt von den ESAs überwachte Anbieter zu wählen, doch kann deren Einstufung als Qualitätsmerkmal im Rahmen der allgemeinen Sorgfaltspflicht der Geschäftsleitung eine Rolle spielen. Gleichzeitig können wirtschaftliche oder strategische Gründe – etwa Preisgestaltung oder spezifische Leistungsanforderungen – gegen die Auswahl eines ESA-kritischen Dienstleisters sprechen.

Die Einführung der ESA-Oversight über kritische IKT-Dienstleister stellt einen echten Paradigmenwechsel in der Regulierung von Drittparteienrisiken dar. Erstmals erhalten die europäischen Aufsichtsbehörden direkte Eingriffsrechte gegenüber externen Technologieanbietern, was die digitale Resilienz des Finanzsektors strukturell stärken soll. Es bleibt aber in der Praxis abzuwarten, ob die ESAs hier auch ausreichendes Knowhow haben oder einholen, um eine praktische IT-Aufsicht durchführen zu können. Eine enge und offene Abstimmung mit der Praxis und den relevanten Dienstleistern ist hier naheliegend und für eine wirksame Aufsicht empfehlenswert.

IV. NIS2 – Überblick, Inhalt und Verhältnis zu DORA

Ziel der NIS2-Richtlinie ist einen gemeinsamen Rechtsrahmen für die Cybersicherheit innerhalb der EU festzulegen, um unionsweit das Sicherheitsniveau gleichmäßig aufzubauen.[24] Indem die Cybersicherheitskapazitäten in der EU gestärkt und Bedrohungen für Netz- und Informationssysteme eingedämmt werden, soll die Sicherheit der Union sowie das stabile Funktionieren der Wirtschaft und Gesellschaft gewährleistet werden.[25]

Der Anwendungsbereich der NIS2-Richtlinie wurde gegenüber ihrer Vorgängerin erheblich erweitert und gilt für eine Vielzahl von Unternehmen, die in verschiedenen Sektoren und Branchen tätig sind (einschließlich digitaler Infrastruktur, Fertigung, Gesundheitswesen, IKT-Dienstleistungsmanagement, Forschung, Verkehr und anderen hochkritischen und kritischen Sektoren).[26] Die NIS2 unterscheidet zwischen sogenannten wesentlichen und wichtigen Unternehmen und erlegt ihnen Cybersicherheitsverpflichtungen in Bezug auf ihre Netz- und Informationssysteme auf, sofern sie die Schwellenwerte für mittlere Unternehmen erreichen oder überschreiten und ihre Dienste in der EU erbringen oder ihre Tätigkeiten dort ausüben.[27] Darüber hinaus gilt die NIS2-Richtlinie für bestimmte Arten von Einrichtungen unabhängig von ihrer Größe, beispielsweise für solche, die gemäß der RL (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden.[28]

Zu den wichtigsten Verpflichtungen gemäß der NIS2-Richtlinie gehören die Registrierung bei den lokalen Cybersicherheitsbehörden, die Umsetzung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, Meldepflichten bei Sicherheitsvorfällen, die Sicherheit der Lieferkette und die Einführung von Governance-Maßnahmen.[29]

Trotz des Ziels, ein einheitliches Cybersicherheitsniveau in der EU zu schaffen, bestehen aufgrund der in der Richtlinie vorgesehenen Mindestharmonisierung[30] weiterhin Unterschiede in der nationalen Gesetzgebung. Dies erschwert in der Praxis eine einheitliche Umsetzung und Anwendung innerhalb der EU. Insbesondere grenzüberschreitend tätige Unternehmen müssen dabei unter Umständen die Umsetzungsgesetze mehrerer Mitgliedstaaten gleichzeitig im Blick behalten.[31]

22) BaFin, Überwachungsrahmen für kritische IKT-Drittdienstleister, https://beck-link.de/f5pky (zuletzt abgerufen am 27.10.2025).
23) Vgl. Lipke BKR 2025, 124 (131 f.).
24) Vgl. Erwgr. 3 ff. NIS2.
25) Vgl. Erwgr. 3 ff. NIS2.
26) Siehe Anhang I „Sektoren mit hoher Kritikalität" und Anhang II „Sonstige kritische Sektoren" zu der NIS2-Richtlinie.
27) Siehe Art. 2 f. NIS2.
28) Siehe Art. 3 Abs. 1 lit. f NIS2.
29) Siehe Art. 3 Abs. 4, 3; Art. 20, 21, 23 NIS2.
30) Siehe Art. 5 NIS2.
31) Karniyevich/Emmerich K&R 2025, 366 (367).

DORA ist lex specialis zur NIS2-Richtlinie und gilt als Verordnung unmittelbar für Finanzunternehmen.[32] In der Praxis bedeutet dies, dass anstelle der NIS2-Bestimmungen die Bestimmungen der DORA gelten, die sich auf Risikomanagement im Bereich der Informations- und Kommunikationstechnologien (IKT), das Management von IKT-bezogenen Vorfällen und insbesondere die Meldung von schwerwiegenden IKT- bezogenen Vorfällen sowie die Prüfung der digitalen Betriebsstabilität, Vereinbarungen über den Informationsaustausch und Risiken durch IKT-Drittanbieter beziehen. Nichtsdestotrotz können in der Praxis Schnittstellen und Überschneidungen auftreten, insbesondere bei Finanzunternehmen und kritischen IKT-Dienstleistern, die zugleich als wesentliche oder wichtige Einrichtungen im Sinne von NIS2 gelten (siehe V).

V. Schnittstellen und Überschneidungen zwischen DORA und NIS2

Die DORA und die NIS2-Richtlinie verfolgen ein gemeinsames Ziel: die Erhöhung der digitalen Resilienz in Europa. Beide Regime beruhen auf ähnlichen Grundprinzipien – insbesondere der Einführung der Governance-Vorgaben, einem risikobasierten Ansatz im Umgang mit Cyberbedrohungen, der Verpflichtung zur Meldung von Sicherheitsvorfälle sowie der Stärkung der Sicherheit der Lieferketten.

Trotz dieser inhaltlichen Parallelen unterscheiden sich die beiden Regelwerke deutlich in ihrer Systematik, Aufsicht und Reichweite. Dies betrifft insbesondere:

- Während DORA als EU-Verordnung unmittelbar gilt und sich gezielt an Finanzunternehmen und deren IKT-Dienstleister richtet, verfolgt NIS2 als Richtlinie den Ansatz einer Mindestharmonisierung und muss von den Mitgliedstaaten in nationales Recht umgesetzt werden.
- Der Anwendungsbereich von NIS2 ist dabei deutlich weiter gefasst: Die Richtlinie erfasst eine Vielzahl von Einrichtungsarten aus unterschiedlichsten Sektoren – von Energie, Verkehr, Gesundheit, Wasser und Abfallwirtschaft bis hin zu digitalen Diensten und digitaler Infrastruktur. In der Praxis bedeutet dies, dass viele in Europa tätige mittelgroße oder große Unternehmen von NIS2 betroffen sein werden.
- DORA hingegen bleibt auf den Finanzsektor und seine kritischen IKT-Dienstleister beschränkt und etabliert ein einheitliches, sektorspezifisches Aufsichtssystem mit zentraler Koordination durch die europäischen Aufsichtsbehörden (EBA, EIOPA, ESMA) und die nationalen Finanzaufsichten. NIS2 sieht dagegen eine dezentrale Aufsicht durch nationale Cyberbehörden vor, die in der Regel sektorenübergreifend zuständig sind.

In der Praxis entstehen Schnittstellen und Überschneidungen vor allem bei Finanzinstituten und kritischen IKT-Dienstleistern, die zugleich als wesentliche oder wichtige Einrichtungen im Sinne von NIS2 gelten. Dies betrifft insbesondere Mischkonzerne und Unternehmensgruppen mit angeschlossenen Zahlungsdienstleistern. Sie müssen unterschiedliche regulatorische Anforderungen erfüllen und gleichzeitig eine einheitliche Cyber- und Compliance-Governance sicherstellen.

Ein zentraler Punkt ist die Meldung von Sicherheitsvorfällen. Sowohl DORA als auch NIS2 enthalten Meldepflichten, die sich jedoch in Definitionen, Schwellenwerten und Meldewegen unterscheiden können. Unternehmen stehen daher vor der Aufgabe, eine kohärente interne Incident-Response-Struktur zu etablieren, die beiden Regimen gerecht wird.

Darüber hinaus erfordert die Umsetzung die Abstimmung technischer und organisatorischer Sicherheitsmaßnahmen. Unterschiedliche Vorgaben in DORA und NIS2 können zu Unsicherheiten führen und erhöhen den Koordinationsaufwand innerhalb der Organisation.

Zugleich eröffnen beide Rechtsakte Chancen für mehr Harmonisierung und Effizienz. Da DORA und NIS2 auf gemeinsamen Grundprinzipien – Cyberresilienz, Risiko-Management, Governance und Incident Reporting – beruhen, können Unternehmen durch integrierte Compliance-Strukturen und abgestimmte Meldeprozesse Synergien schaffen und ihre digitale Widerstandsfähigkeit nachhaltig stärken.

VI. Erste praktische Erfahrungen und offene Fragen aus der Überschneidung von DORA und NIS2

Die gleichzeitige Einführung von DORA und NIS2 hat in der Praxis zu einer Vielzahl von Fragen geführt, insbesondere hinsichtlich der Abgrenzung der Anwendungsbereiche, der Ressourcenplanung und der strategischen Ausrichtung der Cybersecurity-Governance. Während DORA als sektorspezifische Verordnung unmittelbar gilt und für Finanzunternehmen Vorrang vor NIS2 hat (lex specialis), bleibt NIS2 für viele IKT-Dienstleister, insbesondere solche mit kritischen Funktionen, weiterhin relevant. Dies führt zu Doppelregulierungen, etwa bei Meldepflichten, Governance-Anforderungen oder der Bewertung von Drittparteienrisiken. Besonders herausfordernd dürfte die Koordination der Anforderungen bei international tätigen Unternehmen im Hinblick auf NIS2 sein, da die nationale Umsetzung in den EU-Mitgliedstaaten unterschiedlich erfolgt und teils noch aussteht.[33]

Ein zentrales Praxisproblem ergibt sich aus den nationalen Unterschieden bei der Umsetzung von NIS2: Während DORA europaweit einheitlich gilt und zentral durch die europäischen Aufsichtsbehörden koordiniert wird, hängt der Umfang der Pflichten unter NIS2 stark von der jeweiligen nationalen Gesetzgebung und Aufsichtspraxis ab. Dies erschwert die Harmonisierung innerhalb internationaler Unternehmensgruppen und erhöht den Koordinationsaufwand für Compliance- und Security-Teams erheblich.

Aktuelle Entwicklungen der EU weisen auf mögliche Erleichterungen für Unternehmen hin: Die Europäische Kommission hat eine Aufforderung zur Stellungnahme veröffentlicht, um Erfahrungen, Forschungsarbeiten und bewährte Verfahren zur Vereinfachung der Rechtsvorschriften im Rahmen des kommenden digitalen Omnibus zu sammeln. Im Fokus stehen dabei insbesondere Daten, Cybersicherheit und Künstliche Intelligenz (KI). Ziel ist es, den Verwaltungsaufwand zu reduzieren, die Kosten für Unternehmen zu senken und gleichzeitig hohe Sicherheits- und Fairnessstandards beizubehalten. Die Konsultation läuft bis zum 14. Oktober 2025

32) Art. 2 Abs. 10 NIS2.
33) Siehe dazu den NIS2-Umsetzungstracker, https://beck-link.de/28zfh (zuletzt abgerufen am 27.10.2025).

und unterstützt die langfristige Vereinfachungsagenda der EU für digitale Vorschriften.[34]

In den kommenden Monaten ist mit weiteren Konkretisierungen durch nationale Leitlinien, sektorspezifische Prüfanforderungen und ergänzende nationale Gesetze zu rechnen. Viele Unternehmen befinden sich derzeit in einer Übergangsphase, in der Prozesse, Verantwortlichkeiten und Meldeketten neu definiert werden müssen.

Vor diesem Hintergrund empfiehlt sich für Finanzunternehmen und IKT-Dienstleister die Entwicklung einer integrierten, gruppenweiten Cybersecurity-Strategie, die sämtliche regulatorischen Anforderungen von DORA, NIS2 und gegebenenfalls weiterer europäischer sowie nationaler Regelungen umfasst. Anstelle getrennter Compliance-Programme für die jeweiligen Rechtsakte sollte ein gemeinsames Rahmenwerk etabliert werden, das Synergien nutzt, Redundanzen vermeidet und das Sicherheitsniveau nachhaltig stärkt.

Kernbestandteile einer solchen Strategie sind insbesondere:

- Harmonisierung von Meldeprozessen und Incident-Response-Strukturen, um Doppelmeldungen und Inkonsistenzen zu vermeiden;
- Integration von Risikoanalysen für IKT-Dienstleister und Lieferketten in ein einheitliches Risikomanagement;
- Einbindung der Geschäftsleitung in die strategische Steuerung und Überwachung der Cyberresilienz; sowie
- die Nutzung etablierter Standards (zB ISO/IEC 27001, ISO 22301, ISO/IEC 27035) als gemeinsame Grundlage zur Abdeckung beider Regelwerke.

Langfristig bietet die parallele Anwendung von DORA und NIS2 – trotz der zunächst hohen organisatorischen Belastung – auch Chancen für eine stärkere Harmonisierung der europäischen Cybersecurity-Regulierung. Unternehmen, die frühzeitig integrierte Strukturen schaffen, können daraus nicht nur regulatorische Sicherheit, sondern auch einen echten Wettbewerbsvorteil in puncto Resilienz und Vertrauen gewinnen.

VII. Fazit

Mit DORA und NIS2 hat die Europäische Union einen bedeutenden Schritt hin zu einer widerstandsfähigen digitalen Infrastruktur gemacht. Beide Regelwerke markieren einen Paradigmenwechsel: Cybersicherheit und operative Resilienz sind nicht länger reine IT-Themen, sondern zentrale Elemente der Unternehmenssteuerung, Aufsicht und Finanzmarktstabilität. Während DORA den Finanzsektor als systemisch kritischen Bereich gezielt stärkt, sorgt NIS2 für eine sektorübergreifende Anhebung des Sicherheitsniveaus in der europäischen Wirtschaft. Gemeinsam bilden sie den Kern eines europäischen Cyberresilienzrahmens, der bereits jetzt als Vorbild für Regulierungsinitiativen in anderen Ländern dient.

Gleichwohl zeigt die Praxis: Die neuen Regelwerke treffen auf ein bereits hoch reguliertes Umfeld – insbesondere im Finanzsektor. Die teilweise doppelte Regulierung im Bereich IT- und Cybersicherheit verstärkt den ohnehin bestehenden administrativen Aufwand erheblich. Viele Institute sehen sich mit komplexen und teilweise unklar abgegrenzten Anforderungen konfrontiert, die erhebliche Ressourcen binden. Die aktuellen Bestrebungen der Europäischen Kommission und der EZB zur Vereinfachung und Deregulierung – insbesondere im Rahmen des geplanten Digitalen Omnibus und der EZB Task Force zur Vereinfachung der Finanzmarktregulierung[35] – sind daher zu begrüßen und wurden auch von der Praxis sehr positive aufgenommen[36]. Sie sollen nicht nur den Verwaltungsaufwand reduzieren, sondern auch die Kohärenz zwischen Daten-,KI- und Cybersicherheitsvorschriften erhöhen.

Gerade kleinere Institute und Dienstleister stehen vor der Herausforderung, hohe Sicherheitsstandards mit praktikabler Umsetzung in Einklang zu bringen. Denn auch wenn niemand den Wert robuster Cyberresilienz in Frage stellt, fehlt es in der Praxis bislang häufig an Klarheit, Effizienz und Verhältnismäßigkeit der regulatorischen Anforderungen.

Langfristig liegt die Chance jedoch in der Harmonisierung: Unternehmen, die frühzeitig integrierte Governance-,Risiko- und Compliance-Strukturen schaffen, können doppelte Pflichten effizienter erfüllen, regulatorische Risiken minimieren und das Vertrauen von Kunden, Aufsicht und Marktpartnern stärken. DORA und NIS2 stehen damit exemplarisch für den Wandel hin zu einer europäischen Sicherheitskultur, in der digitale Resilienz selbstverständlich wird – und damit zu einem zentralen Stabilitätsfaktor des Finanzsektors der Zukunft.

---

34) Das Digitalpaket wird die Vereinfachungsagenda der Kommission für die kommenden Jahre maßgeblich bestimmen. Basierend auf den Rückmeldungen aus drei öffentlichen Konsultationen soll ein erstes Maßnahmenpaket mit Omnibusvorschriften für den Digitalbereich geschnürt werden, das die Belastung der Unternehmen schnell und spürbar verringern soll. Im Fokus dieser Maßnahmen stehen unter anderem Meldungen von Cybersicherheitsvorfällen. Stellungnahmen können unter folgendem Link eingereicht werden: https://beck-link.de/2n2m8 (zuletzt abgerufen am 27.10.2025) .

35) Vgl. EZB: What is the ECB High-Level Task Force on Simplification?, https://beck-link.de/7ynxh (zuletzt abgerufen am 27.10.2025).

36) Vgl. bspw. Interview mit Karolin Schriever, Vorstand DSGV v. 7. Oktober 2025, https://beck-link.de/vet4y (zuletzt abgerufen am 27.10.2025).