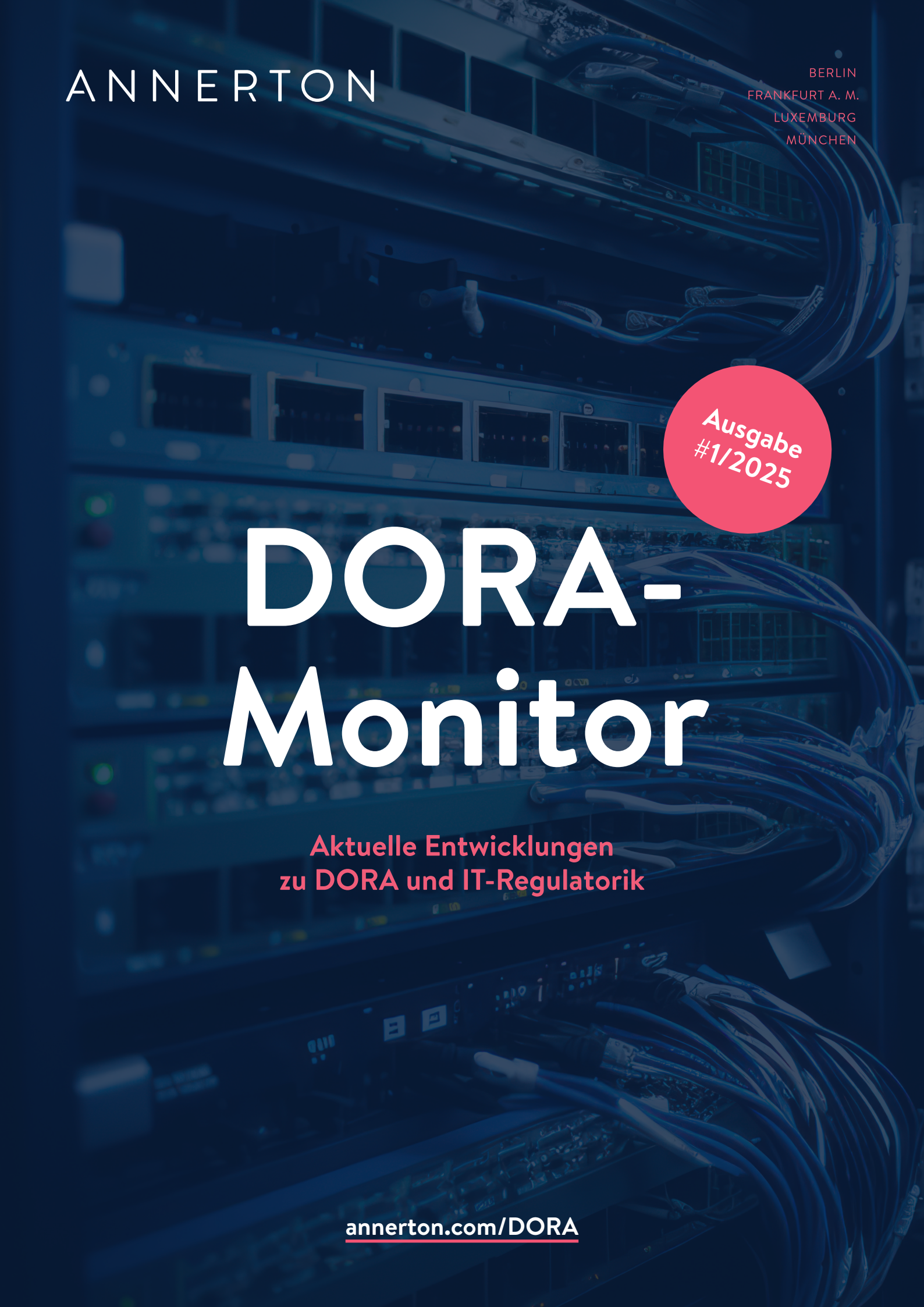
ANNERTON

BERLIN
FRANKFURT A. M.
LUXEMBURG
MÜNCHEN



Ausgabe #1/2025

# DORA-Monitor

## Aktuelle Entwicklungen zu DORA und IT-Regulatorik

annerton.com/DORA

Liebe Leserinnen und Leser,

mit dieser Ausgabe starten wir eine neue Informationsreihe für den Finanzsektor: den DORA-Monitor. Ziel dieser Reihe ist es, Sie regelmäßig, kompakt und praxisorientiert über wesentliche Entwicklungen im Zusammenhang mit der EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) sowie die angrenzende Regulatorik im Bereich IT-Anforderungen zu informieren.

DORA ist nicht nur ein Meilenstein für die europäische Regulierung zu digitaler Resilienz, sondern auch eine erhebliche Herausforderung für Finanzunternehmen in der operativen Umsetzung – insbesondere in Bezug auf die Steuerung von IKT-Risiken, Auslagerungen und Meldepflichten. Die Anforderungen konkretisieren sich derzeit in rasantem Tempo durch RTS, Leitlinien, nationale Klarstellungen und erste Prüfungserfahrungen.

In dieser ersten Ausgabe informieren wir Sie unter anderem über die lang erwartete Veröffentlichung des RTS SUB, der detaillierte Anforderungen an die Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen festlegt. Wir beleuchten zudem die neuesten Aktivitäten der BaFin, insbesondere die aktualisierte Übersicht zu den Mindestvertragsinhalten, die überarbeiteten FAQs zum IKT-Vorfall, sowie die direkte Anwendbarkeit der ESA-Leitlinien zu IKT-Vorfällen.

Ein besonderer Schwerpunkt dieser Ausgabe liegt auf einem Review zur Ersteinreichung des DORA-Informationsregisters aus Sicht der Praxis sowie auf den ersten Erkenntnissen aus den bisher durchgeführten DORA-Audits, die wir aus unserer Beratungspraxis gewonnen haben. Diese Einblicke zeigen, worauf Aufsicht und Prüfer bereits jetzt konkret achten – und welche Fallstricke in der praktischen Umsetzung häufig übersehen werden. Damit erhalten Sie wertvolle Hinweise für die eigene Vorbereitung auf anstehende Prüfungen und eine effektive Ausgestaltung der DORA-Compliance.

Abgerundet wird der DORA-Monitor durch Veranstaltungshinweise und Empfehlungen, damit Sie regulatorisch und strategisch am Puls der Zeit bleiben.

Wir freuen uns, wenn unser DORA-Monitor Ihnen bei der Umsetzung regulatorischer Anforderungen ein verlässlicher und nützlicher Begleiter wird. Für Rückfragen, Diskussionen oder vertiefende Workshops stehen wir Ihnen selbstverständlich jederzeit zur Verfügung.

Ihr
Annerton-Team

# INHALT

Der neue DORA-RTS SUB ist da! ..... 4

BaFin: Aktualisierungen zu DORA ..... 7

1. Aktualisierung der Übersicht zu den Mindestvertragsinhalten nach DORA ..... 7

2. FAQs zum IKT-Vorfall aktualisiert ..... 8

3. ESA-Leitlinien zum IKT-Vorfall direkt anwendbar ..... 9

Review: Ersteinreichung des DORA-Informationsregisters ..... 10

Erste Erkenntnisse aus DORA-Audits ..... 11

Veranstaltungsempfehlungen ..... 13

Über die Autoren ..... 14

Stand dieser Augabe 1/2025: 01.08.2025

# DER NEUE DORA-RTS SUB IST DA!

Die Europäische Kommission hat am 02.07.2025 den technischen Regulierungsstandard (RTS) zur Präzisierung der Aspekte, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss (sog. RTS SUB), formell als Delegierte Verordnung (EU) 2025/532 erlassen. Der RTS SUB legt fest, welche Anforderungen Finanzinstitute bei der Vergabe bzw. Unterauftragsvergabe von IKT-Dienstleistungen erfüllen müssen. Diese sind dann zu beachten, wenn kritische oder wichtige Funktionen bei dem Finanzunternehmen durch eine IKT-Dienstleistung unterstützt werden. Insbesondere kommen die Anforderungen aus dem RTS SUB bei der Risikobewertung und dem Management von IKT-Subdienstleistern zum Tragen.

Im Februar 2025 hatte die Kommission zunächst die Annahme des ursprünglichen Entwurfs des RTS SUB abgelehnt. Der von den Europäischen Aufsichtsbehörden (ESAs) im Juli 2024 vorgelegte Entwurf sah Anforderungen an die „Bedingungen für die Unterauftragsvergabe in der Kette von IKT-Subunternehmern“ vor, die nach Ansicht der Kommission über das in Art. 30 Abs. 5 Unterabsatz 4 DORA festgelegte Mandat hinausging. Die Kommission argumentierte, dass diese Anforderungen nicht spezifisch genug mit den Bedingungen für die Subunternehmervergabe verknüpft waren und somit den Rahmen des Mandats überschritten. Die ESAs waren daher aufgefordert, Artikel 5 sowie die dazugehörige Erwägung 5 aus dem ursprünglichen Entwurf des RTS SUB zu streichen. Dieser Aufforderung sind die ESAs nachgekommen und haben am 24.03.2025 einen aktualisierten Entwurf des RTS SUB vorgelegt, der nunmehr von der Kommission angenommen und veröffentlicht wurde.

Der neue RTS SUB wird nun zum 22.07.2025 wirksam.

## *Praktische Bedeutung des neuen RTS SUB für Finanzunternehmen:*

Der neue RTS SUB konkretisiert und erweitert die in DORA festgelegten Anforderungen an den Einsatz von IKT-Dienstleistungen durch Finanzunternehmen. Ihr Hauptfokus liegt darauf, welche Aspekte ein Finanzunternehmen bei der Weiter- bzw. Untervergabe (Sub-Outsourcing) von IKT-Dienstleistungen berücksichtigen muss, wenn diese Dienstleistungen kritische oder wichtige Funktionen unterstützen. Im Wesentlichen lässt sich die Bedeutung für Finanzunternehmen in folgenden Punkten zusammenfassen:

- **klare Subauslagerungs-Prozesse**
  Der RTS SUB legt detaillierte Kriterien fest, wie Finanzunternehmen Subauslagerungen strukturieren und kontrollieren müssen. Insbesondere müssen klare Prozesse etabliert werden, um sicherzustellen, dass Subdienstleister dieselben Sicherheits-, Datenschutz- und Compliance-Anforderungen erfüllen wie der ursprüngliche Dienstleister.

- **Sorgfaltspflichten und Risikobewertung**
  Finanzunternehmen dürfen nach den Vorgaben des RTS SUB nur dann eine IKT-Dienstleistung an einen Drittdienstleister vergeben, wenn dieser zur kontrollierten und transparenten Untervergabe von IKT-Dienstleistungen zur Unterstützung von kritischen oder wichtigen Funktionen beim Finanzunternehmen befähigt ist und alle aufsichtsrechtlichen Bedingungen erfüllt. Mit dem RTS SUB erhalten Finanzunternehmen nun strengere Vorgaben dazu, wie sie die Risiken im Zusammenhang mit Sub-Outsourcing (zur Unterstützung kritisch-wichtiger Funktionen) identifizieren, bewerten und steuern müssen. Dies betrifft eine ganze Reihe von Risiken (z. B. Ausfall von Systemen), die in Art. 3 Abs. 1 lit. (a) – (j) RTS SUB definiert sind. In die Risikobewertung einfließen müssen u.A.:

  - die Fähigkeit des Hauptdienstleisters, die gesamte Sub-Dienstleisterkette zu identifizieren, um das Finanzunternehmen über diese zu benachrichtigen und zu informieren, und dem Finanzunternehmen alle erforderlichen Informationen zu den eingesetzten Sub-Dienstleistern zur Verfügung zu stellen.
  - die Bewertung der operativen, finanziellen und sicherheitstechnischen Leistungsfähigkeit potenzieller Subunternehmer.
  - die Sicherstellung, dass das Finanzunternehmen und die Behörden vollständige Zugriffs-, Prüfungs- und Informationsrechte entlang der Subunternehmerkette erhält.
  - ausreichende Fähigkeiten, Fachkenntnisse und angemessene finanzielle, personelle und technische Ressourcen beim Hauptdienstleister, um die IKT-Risiken auf der Ebene der Unterauftragnehmer zu überwachen.
  - die Bewertung der Standortrisiken in Bezug auf potentielle Sub-Dienstleister/Sub-Dienstleistungen, der IKT-Konzentrationsrisiken und der Auswirkungen eines möglichen Ausfalls eines Unterauftragnehmers, der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder eines wesentlichen Teils davon erbringt, auf die digitale operationale Resilienz und die finanzielle Solidität des Finanzunternehmens durch das Finanzunternehmen.

  Finanzunternehmen müssen also ihr Risikomanagement in Bezug auf IKT-Dienstleistungen zur Unterstützung kritisch-wichtiger Funktionen vertiefen. Auch regelmäßige Neubewertungen und Aktualisierungen der Risikoanalysen, insbesondere bei Veränderungen an den unterstützten Geschäftsfunktionen, einschließlich IKT-Bedrohungen, IKT-Konzentrationsrisiken und geopolitischen Risiken, müssen implementiert sein.

- **Anforderungen an den Vertrag mit dem Hauptdienstleister**
  Der RTS SUB gibt eine ganze Reihe von Vorgaben dazu, welche Anforderungen an das Sub-Outsourcing und an die vertragliche Vereinbarung hierzu zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister, der kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützt, bestehen. Unter Anderem wird klargestellt, dass

  - der Hauptdienstleister auch im Falle des Sub-Outsourcings verantwortlich bleibt.
  - der Hauptdienstleister die Sub-Dienstleister zu überwachen und die Erfüllung der vertraglichen Verpflichtungen gegenüber dem Finanzunternehmen sicherzustellen hat.

Dazu gehören konkrete Berichtspflichten gegenüber dem Finanzunternehmen.

- der Hauptdienstleister zu einer Risikobewertung in Bezug auf die eingesetzten Sub-Dienstleistern/Sub-Dienstleistungen und den Ort der Datenverarbeitung oder -speicherung durch den eingesetzten Subunternehmer verpflichtet ist.
- der Hauptdienstleister die Kontinuität der IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, entlang der gesamten Kette von Unterauftragnehmern sicherstellen muss, wenn ein IKT-Unterauftragnehmer seinen vertraglichen Verpflichtungen nicht nachkommt.
- das Finanzunternehmen sich vertraglich diverse Durchgriffsrechte (insb. in Bezug auf die Einhaltung von IKT-Sicherheitsstandards, Geschäftsfortführungspläne und Zugangs-/Prüfungsrechte) zusichern lassen muss.

Außerdem legt Art. 6 RTS SUB spezifische Kündigungsrechte fest, die im Zusammenhang mit Sub-Outsourcing zwischen dem Finanzunternehmen und dem Hauptdienstleister zwingend vereinbart werden müssen, wenn kritisch-wichtige Funktionen bei dem Finanzunternehmen oder Teile hiervon unterstützt werden.

- **Umgang mit wesentlichen Änderungen**
  Der neue RTS SUB verpflichtet die Finanzunternehmen, in ihre Verträge mit dem Hauptdienstleister auch aufzunehmen, dass der IKT-Drittdienstleister alle beabsichtigten wesentlichen Änderungen an bestehenden Subunternehmerverträgen, die IKT-Dienstleistungen für kritische oder wichtige Funktionen betreffen, vorab an das Finanzunternehmen mitzuteilen hat. Dies soll dem Finanzunternehmen ermöglichen, die Auswirkungen auf seine Risikoposition und die Leistungsfähigkeit des Hauptdienstleisters rechtzeitig zu bewerten. Der Vertrag muss eine angemessene Frist für die Mitteilung und Prüfung vorsehen. Ohne ausdrückliche Zustimmung oder ausdrückliche Nicht-Ablehnung darf der Dienstleister die Änderungen nicht umsetzen. Erkennt das Finanzunternehmen, dass die geplanten Änderungen seine Risikotoleranz überschreiten, ist es verpflichtet, dies innerhalb der Frist mitzuteilen, die Änderung abzulehnen und ggfs. Anpassungen zu verlangen.

# BAFIN: AKTUALISIERUNGEN ZU DORA

Die BaFin hat in den letzten Wochen eine ganze Reihe von Aktualisierungen zu DORA auf ihrer Webseite https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html veröffentlicht. Im Folgenden gehen wir auf Aktualisierungen ein, die aus praktischer Sicht von hoher Bedeutung sind:

## 1. Aktualisierung der Übersicht zu den Mindestvertragsinhalten nach DORA

Zuletzt am 24.06.2025 hat die BaFin die Übersicht zu den Mindestvertragsinhalten nach DORA erneut aktualisiert und in der aktuellen Fassung auf ihrer Internetseite veröffentlicht.

Die BaFin stellt mit dieser Übersicht den von DORA betroffenen Finanzunternehmen eine Excel-Übersicht dazu zur Verfügung, welche Mindestanforderungen in Verträgen zwischen ihnen und ihren IKT-Drittdienstleistern enthalten sein müssen. Grundlage bilden die Art. 28 – 30 DORA sowie die entsprechenden RTS TPPol (Delegierte VO 2024/1773 vom 13.03.2024 - Technische Regulierungsstandards zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden) und RTS SUB.

### *Was ist neu?*

Die aktuelle Fassung berücksichtigt die folgenden Aspekte:

- **Pflichten im Zusammenhang mit Subauslagerungsketten:**
  Die Vorgaben aus dem neuen RTS SUB, insbesondere zur Vertragsgestaltung im Fall der Beauftragung von Unterauftragnehmern durch IKT-Dienstleister sind in der Tabelle zu den Mindestanforderungen bereits enthalten. Die BaFin hat dazu zwar auf der Grundlage des Entwurfs des neuen RTS SUB gearbeitet, aber im Vergleich mit der nunmehr erlassenen Delegierten Verordnung 2025/532 (neuer RTS SUB) ergeben sich keine inhaltlichen Abweichungen von dem Entwurf des neuen RTS SUB.

  Gemäß Art. 3 (1) lit. b RTS SUB besteht weiterhin die Pflicht des Finanzunternehmens vor Vertragsschluss zu prüfen, ob der IKT-Dienstleister in der Lage ist, alle Sub-Dienstleister in einer Kette von Subauslagerungen zu identifizieren, zu melden und alle Informationen bereit zu stellen. Daneben muss der IKT-Dienstleister während der Vertragsbeziehung die Kontinuität der IKT-Dienstleistung, die kritische oder wichtige Funktionen unterstützt, entlang der gesamten Subauslagerungskette sicherstellen (Art. 4 Abs. 1 lit. g RTS SUB) und

wesentliche Änderungen in den Subauslagerungsvereinbarungen melden (Art. 4 Abs. 1 lit. k RTS SUB).

Gestrichen wurde aber die Pflicht, vertragliche Regelungen mit dem Sub-Dienstleister aufzunehmen, die dem Finanzunternehmen die effektive Überwachung der Dienstleistungen ermöglicht. Die Pflicht zur Vereinbarung von vertraglichen Regelungen zur Bestimmung der Risiken langer Sub-Auslagerungsketten ist ebenfalls entfallen.

Dafür muss aber jetzt gemäß Art. 5 Abs. 1 RTS SUB eine Regelung aufgenommen werden, dass der IKT-Drittdienstleister das Finanzunternehmen rechtzeitig über alle beabsichtigten wesentlichen Änderungen seiner Unterauftragsvereinbarungen informiert, damit das Finanzunternehmen die Auswirkung auf die Risiken, denen er ausgesetzt ist oder ausgesetzt sein könnte, bewerten kann und beurteilen kann, ob solche wesentlichen Änderungen die Fähigkeit des IKT-Drittdienstleisters beeinträchtigen könnten, seinen vertraglichen Verpflichtungen gegenüber dem Finanzunternehmen nachzukommen. Eine entsprechende Mitteilungsfrist ist zu vereinbaren, in der das Finanzunternehmen der Änderung zustimmen oder sie ablehnen kann. Die Änderungen dürfen erst umgesetzt werden, wenn das Finanzunternehmen zugestimmt bzw. sie nicht abgelehnt hat (Art. 5 Abs. 3 RTS SUB).

- **Hinweise zu besonderen Fallgruppen:**
  Neu aufgenommen hat die BaFin Klarstellungen und Hinweise für Finanzunternehmen, die unter den vereinfachten Risikomanagementrahmen im Sinne von Art. 16 Abs. 1 DORA fallen sowie für Kleinstunternehmen im Sinne von Art. 3 Nr. 60 DORA. Dies ist vor allem deshalb relevant, weil der RTS TPPol gemäß Art. 28 Abs. 2 DORA für diese Unternehmen nicht anwendbar ist. Für Kleinstunternehmen sieht Art. 30 Abs. 3 DORA vor, dass zur Wahrnehmung von Zugangs-, Inspektions- und Auditrechten auch ein unabhängiger Dritter beauftragt werden kann, der vom IKT-Drittdienstleister benannt wird. Das Finanzunternehmen, das ein Kleinstunternehmen ist, kann außerdem jederzeit Informationen und Gewähr in Bezug auf die Leistungen des IKT-Drittdienstleisters verlangen.

Unter dem folgenden Link finden Sie die aktuelle Übersicht und weitere Informationen zur Anwendung der neuen Anforderungen auf der Seite der BaFin:
https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/dl_2024_08_05_Mindestvertragsinhalte_DORA_DE_EN.html

## 2. FAQs zum IKT-Vorfall aktualisiert

Die BaFin hat ihre Fragen und Antworten zur Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle am 13.05.2025 aktualisiert. Insbesondere hat die BaFin die Vorgaben der Delegierten Verordnung 2025/301 (RTS zur Festlegung des Inhalts und der Fristen für die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung schwerwiegender IKT-bezogener Vorfälle sowie des Inhalts der freiwilligen Meldung erheblicher Cyberbedrohungen) in ihre FAQs integriert und z.B. herausgestellt, dass eine Erleichterung in Bezug auf die Meldefristen an Wochenenden und Feiertagen gemäß Art. 5 Abs. 4 RTS Meldung gilt, wonach eine Vorfallsmeldung

(Erst-, Zwischen- oder Abschlussmeldung) bis 12 Uhr am nächsten Werktag abgegeben werden darf. Dies gilt allerdings nur für Finanzunternehmen, die weder Kreditinstitute noch zentrale Gegenparteien noch Betreiber von Handelsplätzen noch andere Finanzunternehmen sind, die gemäß den nationalen Vorschriften zur Umsetzung von Art. 3 NIS2 als wesentliches oder bedeutendes Unternehmen bzw. wichtige Einrichtung eingestuft wurden.

## 3. ESA-Leitlinien zum IKT-Vorfall direkt anwendbar

Die BaFin hat im Rahmen ihrer aktuellen Hinweise zur Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle ausdrücklich klargestellt, dass die Gemeinsamen Leitlinien der Europäischen Aufsichtsbehörden (ESA) vom 5. Juni 2024 (JC/GL/2024/34) zur Schätzung der durch schwerwiegende IKT-Vorfälle verursachten aggregierten jährlichen Kosten und Verluste unmittelbar anzuwenden sind.

Unternehmen des Finanzsektors müssen daher die in Titel III der ESA-Leitlinien festgelegten Schätzmethoden für ihre Berichterstattung über IKT-Vorfälle ab sofort beachten. Danach erfolgt die Kostenschätzung durch Aggregation der jährlichen Kosten und Verluste für alle IKT-bezogene Vorfälle, die in ein zu bestimmendes Referenzjahr fallen. Als Referenzjahr kann wahlweise das Kalenderjahr oder das Geschäftsjahr des Unternehmens verwendet werden. Für jeden Vorfall sind Bruttokosten und -verluste sowie etwaige finanzielle Wiedereinziehungen zu ermitteln und zu aggregieren. Die Schätzungen sollen auf Kosten, Verlusten und finanziellen Wiedereinziehungen basieren, die in den Jahresabschlüssen wie der Gewinn- und Verlustrechnung oder gegebenenfalls in den Meldungen des betreffenden Referenzjahres an die Aufsicht ausgewiesen sind. Bei ihrer Schätzung sollten Finanzunternehmen auch buchhalterische Rückstellungen einbeziehen, die in ihren Jahresabschlüssen wie der Gewinn- und Verlustrechnung des betreffenden Referenzjahres ausgewiesen sind.

# REVIEW: ERSTEINREICHUNG DES DORA-INFORMATIONSREGISTERS

Erstmals mussten sämtliche Finanzunternehmen zum 28.04.2025 ihr DORA-Informationsregister über das Meldeportal MVP bei der BaFin einreichen. Die ursprünglich deutlich frühere Frist zum 11.04.2025 konnte nicht eingehalten werden, da erhebliche technische und organisatorische Probleme auf Seiten der BaFin auftraten. Infolgedessen wurde die Einreichungsfrist verlängert und eine Testphase vom 14. bis 28. April 2025 eingerichtet, in der die Institute Rück- und Fehlermeldungen zu ihren Einreichungen erhalten und diese ohne Sanktionen nachbessern konnten.

Die Ersteinreichung war aus Praxissicht von zahlreichen Fehlern und Unklarheiten geprägt. Insbesondere die technischen Anforderungen an das Informationsregister, die sich an den komplexen und EU-weit harmonisierten Vorgaben der ESAs orientieren (müssen), haben dazu geführt, dass die von der BaFin bereitgestellten Vorlagen fehleranfällig und wenig praxistauglich waren. Zum Zeitpunkt der erstmaligen Meldepflicht standen zudem nur unzureichende und schwer verständliche Hilfestellungen bereit, sodass viele Finanzunternehmen erhebliche Schwierigkeiten bei der Umsetzung der Anforderungen an das Informationsregister hatten und wohl bis heute vielfach nicht mit Sicherheit beurteilen können, ob ihre Einreichung den aufsichtsrechtlichen Anforderungen tatsächlich genügt. Auch die Kommunikation zu Format- und Datenspezifika erwies sich als klärungsbedürftig. Insgesamt war der Prozess von Unsicherheiten geprägt und verlief aus Sicht der Praxis keineswegs reibungslos.

Erst sukzessive hat die BaFin ergänzende Ausfüllhinweise und Erklärungen veröffentlicht, die verstärkt zur Klärung des geforderten Formats und der erforderlichen Inhalte beitragen. Eine finale Bewertung und echte Praxiserkenntnisse sind jedoch wohl erst möglich, wenn die Europäischen Aufsichtsbehörden (ESAs) die erste Auswertung der eingereichten Informationsregister abgeschlossen und etwaige Rückmeldungen oder Präzisierungen veröffentlicht haben. Bis dahin verbleibt für viele Institute noch eine erhebliche Rechts- und Umsetzungssicherheit.

# ERSTE ERKENNTNISSE AUS DORA-AUDITS

Die BaFin und die Bundesbank haben damit begonnen, ein erstes Lagebild zum Umsetzungsstand von DORA durch angeordnete IT-Prüfungen zu erheben. Erste Berichte aus bereits durchgeführten DORA-Prüfungen zeichnen ein konsistentes Bild der bestehenden Herausforderungen bei der praktischen Umsetzung von DORA.

- **IKT-Risikomanagement als ein Schwerpunkt:** Zu den ersten praktischen Erkenntnissen aus durchgeführten DORA-Audits lässt sich festhalten, dass ein starker Fokus der Aufsicht auch auf der Schaffung transparenter und praxistauglicher Prozesse für das IKT-Risikomanagement liegt. Erste Erfahrungen zeigen bereits, dass die etablierten internen Kontrollmechanismen, insbesondere in den Bereichen kontinuierliches Monitoring, Notfallplanung und Auslagerungsmanagement, im Mittelpunkt der Prüfungen stehen. Die Beobachtungen der ersten Audits deuten zudem darauf hin, dass Aufsichtsbehörden insbesondere auf die Qualität der Risikoanalyse, die Aktualität der Bestandsaufnahmen und die klare interne Verantwortungszuweisung Wert legen.

- **keine Individualisierung:** Auffällig ist, dass viele Institute bislang die DORA-Anforderungen zwar formal in ihre internen Richtlinien und Prozesse überführen – oftmals sogar mit nahezu wörtlicher Übernahme der gesetzlichen Vorgaben –, diese aber nicht ausreichend an die individuellen Gegebenheiten und spezifischen Risiken des eigenen Instituts anpassen. Dies wird von den Prüfern regelmäßig kritisch angesprochen und als fehlende Umsetzungstiefe bewertet.

- **fehlende Definitionen:** Ein weiteres Problemfeld betrifft die Definition und Abgrenzung zentraler Begriffe sowie die einheitliche Anwendung in den Prozessen. Begriffe wie „Anomalie“ oder „IKT-Vorfall“ werden vielfach nicht eindeutig voneinander abgegrenzt, was Unsicherheiten bei der Kategorisierung, Meldepflicht und der weiteren Behandlung der Vorfälle innerhalb des Instituts verursacht.

- **Rollen, Zuständigkeiten und Verantwortlichkeiten** sind oft unklar oder nicht ausreichend eindeutig zugeordnet, was zu erheblichen Organisations- und Steuerungsdefiziten führt.

- **technischer Prüfungsmaßstab:** In technischer Hinsicht orientieren sich die Prüfer offenbar stark den dem IT-Standard des BSI (BSI IT-Grundschutz), sodass die Anforderungen im Bereich Informationssicherheit, Risikomanagement und technischer Organisation eng an diesen Standard angelehnt werden. Insbesondere werden Prozesse und Maßnahmen im Bereich IKT-Sicherheit, Governance und Dokumentation anhand der vom BSI etablierten Schutzziele analysiert.

- **Klassifizierung von IKT-Assets:** Herausfordernd gestaltet sich zudem für die Praxis die Einstufung von „kritischen oder wichtigen Funktionen“ im Sinne von DORA und deren Übertragung auf sämtliche bestehende IKT-Assets und IKT-Dienstleister. Hier fehlt es häufig an einer systematischen und vollständigen Anwendung der Vorgaben, was die Risikosteuerung und die Einhaltung aufsichtsrechtlicher Anforderungen erschwert.

- **Verträge mit IKT-Dienstleistern:** Erheblich Defizite werden auch bei den Verträgen mit IKT-Dienstleistern festgestellt. Viele Verträge entsprechen nicht den Mindestanforderungen nach Art. 30 Abs. 2 und Abs. 3 DORA und es besteht für die Praxis auch noch wenig Klarheit darüber, welche konkreten Dienstleistungen als IKT-Dienstleistungen nach DORA einzustufen sind. Die Anforderungen an den Umgang mit oftmals in der Praxis genutzten Full-Service-Lösungen, die teilweise IKT-Dienstleistungen beinhalten und teilweise auch Non-IT-Leistungen liefern, sind unklar. Auch hier bestehen in der Praxis noch deutliche Unsicherheiten und teils erhebliche Lücken.

Einzelfallbezogene Ergebnisse und Rückmeldungen aus bereits abgeschlossenen Audits sind bisher, auch aufgrund der Sensibilität der Thematik und der relativen Neuheit der Regulierung, nicht öffentlich dokumentiert. Die Rechtspraxis beobachtet jedoch bereits, dass Unternehmen proaktiv strategische und operative Anpassungen ihrer IKT-Governance vornehmen, um regulatorischen Anforderungen von DORA weiter gerecht zu werden.

Zusammenfassend zeigen die bisherigen DORA-Prüfungen, dass erheblicher Aufwand im Bereich individuelle Anpassung, Begriffsdefinition und organisationsspezifischer Ausgestaltung der Dokumentation besteht. Die Aufsicht legt bei den Prüfungen nicht nur Wert auf die formale Übernahme von DORA-Anforderungen, sondern insbesondere darauf, dass diese auf das jeweilige Institut praxisgerecht und risikoadäquat übertragen werden – und dass Begriffe, Verantwortlichkeiten und Abläufe eindeutig, nachvollziehbar und konsistent ausgestaltet sind.

Für die Praxis wäre es äußerst hilfreich, wenn die Aufsichtsbehörden ihre Erwartungshaltung hinsichtlich der Auslegung und Umsetzung der DORA-Anforderungen analog der ehemaligen xAIT in präzisierenden Veröffentlichungen konkretisieren würden. Eine solche Klarstellung würde den Finanzunternehmen eine verlässlichere Orientierung bei der praktischen Umsetzung der regulatorischen Vorgaben bieten und Unsicherheiten im Audit-Prozess wirksam reduzieren. Wir gehen davon aus, dass die gesammelten Erkenntnisse aus den schon durchgeführten und künftig anstehenden DORA-Prüfungen von der Aufsicht ausgewertet und in Form entsprechender Veröffentlichungen kommuniziert werden. Dadurch könnten Best-Practice-Ansätze, typische Herausforderungen sowie aufsichtsrechtliche Schwerpunkte für die Branche transparent gemacht und die Umsetzung der DORA-Anforderungen weiter vereinheitlicht und erleichtert werden. Mit ihren Hinweisen zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement und auch schon mit ihrer Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter hat die BaFin bereits begonnen, dies entsprechend umzusetzen.

# VERANSTALTUNGSEMPFEHLUNGEN

## Wir laden Sie ein zur Webcastreihe #FitfürDORA


In unserer kostenfreien Online-Reihe #FitfürDORA gibt Rechtsanwältin und Fachanwältin für IT-Recht Josefine Spengler praxisnahe Einblicke, wie sich typische Herausforderungen im Kontext der Digital Operational Resilience meistern lassen.
Ziel der Veranstaltungsreihe ist es, einen offenen Austausch aus der Praxis für die Praxis zu fördern.

**Format:** Online via Microsoft Teams
**Teilnahme:** Kostenfrei, Anmeldung erforderlich
**Informationen:** https://annerton.com/dora/webcast/

DIE NÄCHSTEN TERMINE UND THEMEN:

| | | |
|---|---|---|
| 26.9. | IKT-Drittparteien im Fokus von DORA | Freitag, 26. September 2025, 11 – 12 Uhr<br>Anmeldung & Informationen |
| 21.11. | IKT-Risikomanagement-rahmen nach DORA | Freitag, 21. November 2025, 11 – 12 Uhr<br>Anmeldung & Informationen |

ONLINE-SEMINAR DES FORUM-INSTITUT
MIT DEN ANNERTON-ANWÄLTEN
PETER FREY UND JOSEFINE SPENGLER

## DORA in der Praxis


In diesem Online-Seminar werden Ihnen die regulatorischen Erwartungen der Aufsicht von unseren Experten für IT-Recht, Bank- & Bankaufsichtsrecht, Finanzdienstleistungsrecht und Auslagerungsmanagement erläutert.

Außerdem erfahren Sie, welche Vorgaben an die IT von Finanzunternehmen unter DORA gelten. Dabei erhalten Sie Umsetzungstipps und Hilfestellungen, insbesondere für das Dauerbrenner-Thema „Outsourcing". Abschließend erfahren Sie aus der Perspektive der Wirtschaftsprüfung die vorliegenden Erkenntnisse aus der bisherigen Umsetzung sowie die Auswirkungen auf die Abschlussprüfung 2025.

**Termin:** Montag, 20. Oktober 2025, 9 – 17 Uhr
**Ort:** Online, FORUM INSTITUT
**Anmeldung:** https://www.forum-institut.de/seminar/25103011-dora-in-der-praxis

# ÜBER DIE AUTOREN


## Josefine Spengler

RECHTSANWÄLTIN
FACHANWÄLTIN FÜR IT-RECHT
COUNSEL

T +49 30 863 21 88-26
E JSpengler@annerton.com
Vollständiges Profil



## Peter Frey

RECHTSANWALT
PARTNER

T +49 89 306 683 -215
E PFrey@annerton.com
Vollständiges Profil


Kontaktieren Sie uns unter
**DORA@annerton.com**