www.compliance-berater.de

Compliance Berater

1-2 / 2023

Betriebs-Berater Compliance

19.1.2023 | 11.Jg
Seiten 1–48

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Dr. Thorsten Ammann und Yannick Zirnstein*

DORA – IT-Sicherheit gesetzlich verordnet

Das Gesetzgebungsverfahren zum „Digital Operations Resilience Act" („DORA") ist durch die Annahme des Europäischen Rats am 28.11.2022 abgeschlossen. Regelungsgegenstand ist die Stärkung der digitalen operativen Resilienz von im Finanzsektor tätigen Unternehmen zur bestmöglichen Vermeidung von Cyberbedrohungen und zum angemessenen Umgang mit diesen. Für diese Zwecke bringt DORA als erstes europäisches branchenspezifisches Gesetz zur IT-Sicherheit eine Fülle unterschiedlicher Pflichten für zahlreiche Marktteilnehmer mit sich, deren Erfüllung mit hohen Aufwänden verbunden sein wird, die aber zugleich das Potential mit sich bringen, einen neuen Marktstandard zu etablieren. DORA tritt bereits am 16.1.2023 in Kraft. Die Vorgaben sind bis zum 17.1.2025 von den Regelungsadressaten umzusetzen.

I. Einleitung

DORA[1] legt branchenspezifisch für im Finanzsektor tätige Unternehmen neue einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen fest (Art. 1 Abs. 1 DORA). Es sollen detaillierte und umfassende Mindestanforderungen, insbesondere hinsichtlich des Risikomanagements im Bereich der Informations- und Kommunikationstechnologie (IKT) und des IKT-Drittparteienmanagements etabliert werden. Umfangreiche Aufgaben und Befugnisse der mit der Überwachung der Einhaltung von DORA betreuten Aufsichtsbehörden, sowie ausführliche Meldepflichten im Falle von IKT-bezogenen Vorfällen vervollständigen den Pflichtenkanon. Dieser Artikel befasst sich mit den wesentlichen Inhalten von DORA. Hierfür werden zunächst die Hintergründe und Regelungsziele des Gesetzes erläutert (Abschnitt II). Daran schließt sich eine Übersicht über die Normadressaten (Ziffer III) und deren gesetzliche Pflichten (Ziffer IV) an, insbesondere im Hinblick auf das Risikomanagement im Zusammenhang mit IKT-Drittdienstleistern (Ziffer V). Das Ende des Artikels bilden ein Fazit, das sich mit den Herausforderungen für Unternehmen und Regulierungspraxis beschäftigt, sowie einige Handlungsempfehlungen (Ziffer VI).

II. Hintergründe und Regelungsziele

Ziel von DORA ist es, vor dem Hintergrund stetig steigender Cybersicherheitsrisiken[2] im Finanzsektor europaweit einheitliche Regelungen zu etablieren, um die IT-Sicherheit im europäischen Binnenmarkt auf ein einheitliches Niveau anzuheben.[3] Der Vielzahl derzeit anzutreffender nationaler Regulierungsinitiativen und Aufsichtskonzepte auf Ebene der Mitgliedstaaten kommt angesichts des grenzüberschreitenden Charakters von IKT-Risiken nur eine begrenzte Wirkung zum Schutz gegen Cyberattacken zu. Auch haben unter den Mitgliedstaaten nur unzureichend abgestimmte nationale Alleingänge in der Vergangenheit zu Überschneidungen, Inkohärenzen, Inkonsistenzen und erheblichen administrativen Mehraufwänden und Mehrkosten – insbesondere für grenzüberschreitend tätige Finanzunternehmen – oder dazu geführt, dass IKT-Risiken nur unzureichend erkannt oder gar nicht erst angegangen werden konnten.[4]

Dem soll DORA entgegenwirken. Hierzu führt DORA detaillierte und umfassende Mindestanforderungen, insbesondere hinsichtlich des Risikomanagements im Bereich der Informations- und Kommunikationstechnologie (IKT) und des IKT-Drittparteienmanagements, ein. Demnach sollen sämtliche Regelungsadressaten über Sicherheitsvorkehrungen verfügen, die ihre digitale Betriebsstabilität stärken, Cyber-Angriffe und andere IT-Risiken rechtzeitig erkennen und ihre Auswirkungen verlässlich mindern. Um dies zu erreichen, sieht DORA verschiedene Standards sowie Regelungen für eine effizientere Koordinierung und Beaufsichtigung betroffener Unternehmen vor. Hierzu gehört u. a., dass IKT-Systeme regelmäßig zu prüfen[5] und Sicherheitsvorfälle künftig zu melden sind.[6] Auch sollen zuständige Aufsichtsbehörden von erweiterten Befugnissen profitieren, insbesondere um auch solche Risiken verlässlich überwachen und steuern zu können, die sich aus oder im Zusammenhang mit der Abhängigkeit von Finanzunternehmen von eingeschalteten IKT-Drittdienstleistern, beispielsweise im Rahmen von Auslagerungen oder Ausgliederungen (Outsourcing), ergeben.[7] Insoweit trifft DORA zumindest mittelbar auch IT Services Provider.[8]

* Die Autoren danken Herrn Constantin Orth (wissenschaftlicher Mitarbeiter) für die hilfreiche Unterstützung im Zusammenhang mit der Abfassung dieses Beitrags.

1 Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6 (Abrufdatum: 5.12.2022).

3 ErwG 11 zu DORA.

4 DORA orig. Entwurf vom 24.9.2020, S.1.

5 Abschnitt IV.3.

6 Abschnitt IV.4.

7 Abschnitt V.3.c).

8 Abschnitt V.

III. Adressaten

Die Verordnung richtet sich an einen breiten Kreis von im Finanzsektor tätigen Unternehmen (vgl. Art. 2 Abs. 1 DORA). Hierzu zählen Finanzunternehmen wie Banken, Wertpapierfirmen, Handelsplätze, Versicherungs- und Rückversicherungsunternehmen (vgl. Art. 2 Abs. 2 DORA), aber auch IKT-Dienstleister (Art. 2 Abs. 1 lit. u) DORA).
Vom Anwendungsbereich ausgenommen sind eine kleine Anzahl von im Finanzsektor tätigen Unternehmen, wie beispielsweise Verwalter alternativer Investmentfonds im Sinne des Art. 3 Abs. 2 RL 2011/61/EU[9], oder Versicherungs- und Rückversicherungsunternehmen im Sinne des Art. 4 RL 2009/138/EG[10] (Art. 2 Abs. 3 DORA). Abschlussprüfungsgesellschaften sind ebenso nicht erfasst. Sie werden jedoch Teil einer künftigen Überprüfung von DORA sein, bei der die Notwendigkeit einer möglichen Überarbeitung der Vorschriften untersucht werden soll (Art. 58 Abs. 3 DORA).
Die Mitgliedsstaaten können zudem die in Art. 2 Abs. 5 Nr. 4–23 RL 2013/26/EU[11] genannten Stellen vom Anwendungsbereich der DORA ausschließen. Für Deutschland kämen die „Kreditanstalt für Wiederaufbau", sowie Unternehmen, die aufgrund des Wohnungsgemeinnützigkeitsgesetzes als Organe der staatlichen Wohnungspolitik anerkannt sind und nicht überwiegend Bankgeschäfte betreiben und Unternehmen, die aufgrund dieses Gesetzes als gemeinnützige Wohnungsunternehmen anerkannt sind, in Betracht (Art. 2 Abs. 5 Nr. 6 RL 2013/26/EU).
Der Anwendungsbereich von DORA ist mithin weit. Der europäische Gesetzgeber erkennt aber auch, dass die strengen Vorgaben nicht unbedingt für alle Finanzunternehmen gleichermaßen gelten können. Hierfür bietet der gesetzlich festgelegte Verhältnismäßigkeitsgrundsatz und risikobasierte Ansatz das erforderliche Korrektiv und erlaubt es Finanzunternehmen, auf der Basis von Faktoren wie etwa der Unternehmensgröße und des Risikoprofils, die Art und Weise der Umsetzung der Vorgaben bedarfs- und interessengerecht festzulegen (Art. 4 DORA).[12]

IV. Neue Anforderungen an Compliance

1. Gesamtverantwortlichkeit der Geschäftsleitung

Für sämtliche Pflichten im Zusammenhang mit dem IKT-Risikomanagements (Art. 5 Abs. 2 DORA) sowie der Gesamtstrategie für die digitale operationale Resilienz ist das jeweilige Leitungsorgan des Finanzunternehmens gesamtverantwortlich.
Aus der Gesamtverantwortlichkeit des Leitungsorgans folgt zunächst die Pflicht zur Einrichtung eines internen Governance- und Kontrollrahmens (Art. 5 Abs. 1 DORA). Hierfür definiert DORA mehrere Voraussetzungen, die das Leitungsorgan erfüllen muss: Unter anderem hat das Leitungsorgan Aufgaben und Verantwortlichkeiten für IKT-bezogene Funktionen und Governance-Regelungen zu definieren (Art. 5 Abs. 2 lit. c) DORA) und Meldekanäle für bestimmte Informationen einzurichten (Art. 5 Abs. 2 lit. i) DORA).

2. IKT-Risikomanagement

Finanzunternehmen haben als Bestandteil ihres Gesamtrisikomanagementsystems einen „soliden, umfassenden" IKT-Risikomanagementrahmen zu implementieren. Dieser soll es ermöglichen, IKT-Risiken angemessen zu begegnen und ein hohes Niveau an digitaler operativer Resilienz zu gewährleisten (Art. 6 Abs. 1 DORA). Zu den Mindestinhalten des IKT-Risikomanagementrahmens zählen Strategien, Richtlinien, Verfahren, Protokolle und Anwendungen, die erforderlich sind, um alle Informations- und IKT-Assets umfassend und angemessen vor negativen Beeinträchtigungen gleich welcher Art zu schützen (Art. 6 Abs. 2 DORA). Liegt der IKT-Risikomanagementrahmen vor, ist er in mindestens einjährigen Abständen zu überprüfen und gegebenenfalls anzupassen (Art. 6 Abs. 5 DORA) sowie regelmäßig einer internen Revision zu unterziehen (Art. 6 Abs. 6 DORA).
An dieser Stelle ist der Verhältnismäßigkeitsgrundsatz und der zugrundeliegende risikobasierte Ansatz deutlich zu erkennen. Dies liegt zunächst an der Abstraktheit der Vorgaben zum IKT-Risikomanagementrahmen, die unter Berücksichtigung der Unternehmensprozesse und dafür eingesetzten technischen Mittel individuell zu konkretisieren sind. Diese Abstraktheit wird zudem durch die Verwendung zahlreicher unbestimmter Rechtsbegriffe, wie etwa die Gewährleistung eines „angemessene[n] Schutz[es] aller Informations- und IKT-Assets" (Art. 6 Abs. 2 DORA), nochmals deutlich erhöht. Im Rahmen dieses Beispiels wären also zunächst alle Informations- und IKT-Assets zu identifizieren und es wäre zu prüfen, welchen Schutz diese benötigen. Schließlich würde sich die Frage stellen, welches Schutzniveau dann „angemessen" wäre.
Für bestimmte (kleinere) Unternehmen gelten insoweit vereinfachte Anforderungen (Art. 16 DORA).

3. Resilienzanforderungen und Prüfpflichten, inkl. Threat Lead Penetration Testing

Zur Gewährleistung eines kontinuierlich hohen Schutzniveaus, das mit technologischen Neuerungen Schritt halten kann, sollen Finanzunternehmen ihre digitale Betriebsstabilität ständig auf den Prüfstand stellen (Art. 24–27 DORA).

a) Allgemeine Anforderungen

Finanzunternehmen haben gemäß DORA ein weitreichendes Programm zur Überprüfung ihrer digitalen Betriebsstabilität zu entwickeln, um ihre Abwehrbereitschaft zu bewerten, Schwachstellen, Mängel oder Lücken in ihrer digitalen Betriebsstabilität zu erkennen und Korrekturmaßnahmen frühzeitig umsetzen zu können (Art. 24 Abs. 1 DORA). Die spezifische Gestaltung dieses Programms liegt erneut im Ermessen der Finanzunternehmen, die auch insoweit zu einem risikobasierten Ansatz verpflichtet sind (Art. 24 Abs. 3 DORA).[13]
Finanzunternehmen haben zudem sicherzustellen, dass die Prüfungen von unabhängigen internen oder externen Parteien durchgeführt werden. Bei internen Prüfern müssen die Finanzunternehmen ausreichende Ressourcen bereitstellen und sicherstellen, dass Interes-

9 Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 über die Verwalter alternativer Investmentfonds und zur Änderung der Richtlinien 2003/41/EG und 2009/65/EG und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 1095/2010.
10 Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II).
11 Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG.
12 Vgl. auch ErwG 13, 36 zu DORA.
13 ErwG 56 zu DORA.

senkonflikte während der gesamten Planungs- und Durchführungsphase des Tests vermieden werden (Art. 24 Abs. 4 DORA).[14]

b) Umfang und Ausmaß der Prüfung

Der Prüfrahmen orientiert sich an Größe und Geschäfts- und Risikoprofil eines Finanzunternehmens. Umfang und Frequenz der Prüfung richten sich am Schutzbedarf und dem ausgesetzten Risiko der einzelnen IKT-Systeme aus.

Welche Art der Prüfung unter welchen Umständen angemessen und erforderlich ist, liegt im Ermessen des Finanzunternehmens. Mögliche Verfahren sind beispielsweise Schwachstellenbewertungen und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Überprüfungen der physischen Sicherheit, Quellcodeprüfungen, Kompatibilitätstests und Penetrationstests (Art. 25 Abs. 1 DORA).

c) Durchführung von Penetrationstests

Einzelne Finanzunternehmen haben abhängig von bestimmten Kriterien, in mindestens dreijährigen Abständen von Testern bedrohungsgeleitete Penetrationstests (threat lead penetration testing) („TLPT") im Funktionsmodus durchzuführen. Die Regelmäßigkeit dieser TLPT kann je nach Risikoprofil des jeweiligen Finanzunternehmens variieren (Art. 26 Abs. 1 DORA).

Sofern davon auszugehen ist, dass IKT-Drittdienstleister und/oder Kunden durch die Durchführung des TLPT betroffen sein könnten, sind zusätzliche Sicherheitsmaßnahmen erforderlich (Art. 26 Abs. 3, 4 DORA).

Die genaue Vorgehensweise, Umfang von TLPT und die Testmethodik sind von den europäischen Aufsichtsbehörden (ESA) und der EZB zu definieren, wobei ein Einklang mit dem bereits existierenden TIBER-EU[15]-Standard erreicht werden soll (Art. 26 Abs. 11 DORA).

4. Sicherheitsvorfälle und Meldepflichten

a) Anforderungen an Finanzunternehmen

Finanzunternehmen haben einen Prozess zur Überwachung, Protokollierung und Meldung IKT-bezogener Vorfälle einzurichten (Art. 17 Abs. 1 DORA). Vorfälle und Auswirkungen sind zur Festlegung von Wesentlichkeitsschwellen nach bestimmten Kriterien zu klassifizieren (Art. 18 DORA). Schwerwiegende Vorfälle müssen, signifikante Vorfälle können bei erhöhter Bedrohungsrelevanz den Finanzaufsichtsbehörden gemeldet werden (Art. 19 Abs. 1, 2 DORA). Durch verpflichtende Berichte sind Kunden und Nutzer der Finanzunternehmen über Vorfälle und deren Auswirkungen zu informieren (Art. 19 Abs. 3 DORA). Die Auslagerung der Wahrnehmung der Meldepflichten ist auch hier unter Beibehaltung der Gesamtverantwortungsübernahme möglich (Art. 19 Abs. 5 DORA).

Schwellenwerte für die Wesentlichkeit einer Meldepflicht, sowie präzise Anforderungen an den Inhalt und die Frist für eine Meldung sind bislang nicht genau festgelegt.[16] Hierfür sollen die Finanzaufsichtsbehörden ein einheitliches Meldeformular und technische Standards ausarbeiten.[17]

b) Kooperation mit Behörden

Aufsichtsbehörden haben im Anschluss an eine Meldung, zeitnah sachdienliche Rückmeldungen zu geben oder allgemeine Orientierungshilfen für das Finanzunternehmen bereitzustellen (Art. 22 Abs. 1 DORA). Die Finanzunternehmen bleiben trotz dessen für den Umgang mit dem Vorfall und dessen Folgen vollumfänglich verantwortlich.

V. Anforderungen an die Einbindung von IKT-Drittdienstleistern

Als Teil des Risikomanagementprozesses etabliert DORA teils neue, teils bereits aus den Leitlinien zu Auslagerungen der European Banking Authority (EBA-Leitlinien)[18] bekannte[19] Anforderungen zur Erfassung von Risiken im Zusammenhang mit der Einbindung von IKT-Drittdienstleistern (Art. 28 bis 44 DORA). Finanzunternehmen haften jederzeit und in vollem Umfang für die Einhaltung und Erfüllung sämtlicher Verpflichtungen der Verordnung durch von ihnen beauftragten Drittdienstleister (Art. 28 Abs. 1 lit. a) DORA). Es ist ein Informationsregister mit sämtlichen ausgelagerten IKT-Prozessen zu pflegen (Art. 28 Abs. 3 DORA). Finanzunternehmen müssen im Allgemeinen eine vollumfängliche (von Vertragsabschluss bis zur Nachvertragsphase) Überprüfung und Überwachung der betreffenden IKT-Drittdienstleister gewährleisten (Art. 28-30 DORA).

1. Definition

DORA fasst den Begriff des IKT-Drittdienstleisters weit und definiert diesen als jedes „Unternehmen, das IKT-Dienstleistungen bereitstellt" (Art. 3 Nr. 19 DORA). IKT-Dienstleistungen beinhalten „digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste (Art. 3 Nr. 21 DORA)." Von der Begrifflichkeit erfasst sind daher u. a. Entwickler von Banking-Apps, Hersteller von Geldautomaten und Betreiber von Kernbankensystemen ebenso wie klassische IT-Service Provider.

2. Allgemeine Anforderungen

Von einzelnen Ausnahmen abgesehen, müssen Finanzunternehmen als festen Bestandteil ihres IKT-Risikomanagements eine Strategie für den Umgang mit Risiken, die aus oder im Zusammenhang mit der Einbindung von IKT-Drittdienstleistern resultieren, beschließen und diese Strategie regelmäßig überprüfen (Art. 28 Abs. 2 DORA). Die Strategie hat auch eine Leitlinie zur Einbindung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, zu umfassen. Zu sämtlichen ausgelagerten IKT-Prozessen und den damit zusammenhängenden vertraglichen Vereinbarungen ist ein Informationsregister zu erstellen und zu pflegen und auf Anfrage der zuständigen Behörde vorzulegen (Art. 28 Abs. 3 DORA). Die zuständigen Behörden sind mindestens einmal jährlich zur Anzahl neuer Vereinbarungen über die Nutzung von IKT-Dienstleistungen, den Kategorien der eingebundenen IKT-Drittdienstleister, der Art der vertraglichen Vereinbarungen

14 ErwG 61 zu DORA.

15 Die Abkürzung TIBER-EU steht für „Threat Intelligence-based Ethical Red Teaming" und steht für einen Rahmen, der einen kontrollierten, einzelfallbezogenen Red-Team-Test der kritischen Live-Produktionssysteme von Unternehmen ermöglicht.

16 Vgl. ErwG 23 zu DORA.

17 ErwG 100 zu DORA.

18 European Banking Authority, Leitlinien zu Auslagerungen vom 25. Februar 2019, EBA/GL/2019/02, abrufbar unter https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/5546a705-bff2-43eb-b382-e5c7bed3a2bc/EBA%20revised%20Guidelines%20on%20outsourcing_DE.pdf?retry=1 (Abrufdatum: 4.12.2022).

19 Hierzu auch *Arkat/Müller*, BKR 2021, 424, 429.

sowie den bereitgestellten IKT-Dienstleistungen und -Funktionen zu informieren. Auch sind die zuständigen Behörden über jede geplante vertragliche Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sowie in dem Fall, dass eine Funktion kritisch oder wichtig geworden ist, zu unterrichten.

3. Maßnahmen vor Einbindung eines IKT-Drittdienstleisters

Regelungsadressaten[20] haben vor Abschluss einer vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen insbesondere die folgenden wesentlichen Anforderungen zu erfüllen:

a) Auswahlprozess und Risikenevaluierung

Nach Art. 28 Abs. 4 DORA haben Finanzunternehmen zunächst sorgfältig zu evaluieren, ob und inwieweit die Einbindung des jeweiligen IKT-Drittdienstleisters eine Funktion betrifft, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten oder Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen oder -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach den anwendbaren finanzrechtlichen Bestimmungen erheblich beeinträchtigen würde (Art. 28 Abs. 4 lit. a), 3 Abs. 22 DORA). Darüber hinaus ist zu beurteilen, ob die aufsichtsrechtlichen Bedingungen für die Auftragsvergabe erfüllt sind (Art. 28 Abs. 4 lit. b) DORA). Ferner sind sämtliche im Zusammenhang mit der beabsichtigten vertraglichen Vereinbarung mit dem IKT-Drittdienstleister einhergehenden relevanten Risiken einschließlich des Umstands, inwieweit in Art. 29 DORA genannte IKT-Konzentrationsrisiken[21] hierdurch erhöht werden, zu ermitteln und zu bewerten (Art. 28 Abs. 4 lit. c) DORA).

Für eine solche Risikoerhöhung kann insbesondere sprechen, dass der betreffende IKT-Drittdienstleister nicht ohne Weiteres ersetzbar ist (Art. 29 Abs. 1 lit. a) DORA), oder der betreffende IKT-Drittdienstleister bereits in andere kritische oder wichtige Funktionen eingebunden worden ist (Art. 29 Abs. 1 lit. b) DORA). Dies gilt u. a. auch dann, wenn beabsichtigt ist, dem betreffenden IKT-Drittdienstleister auch die Möglichkeit zur Vergabe von Unteraufträgen einzuräumen (Art. 29 Abs. 2 DORA). In diesem Fall ist zudem stets ein Augenmerk auf die Einhaltung der geltenden datenschutzrechtlichen Bestimmungen zu legen, insbesondere wenn nicht ausgeschlossen werden kann, dass personenbezogene Daten im außereuropäischen Ausland verarbeitet werden oder ein Zugriff von dort nicht sicher ausgeschlossen werden kann (Art. 29 Abs. 2 DORA). Obwohl die Vereinbarung der Unterauftragsvergabe unter Berücksichtigung geltender datenschutzrechtlicher Bestimmungen grundsätzlich zulässig ist, ist stets auch zu evaluieren, ob und inwieweit sich potenziell lange oder komplexe Ketten der Unterauftragsvergabe negativ auf die Steuerung und Überwachung der vertraglich vereinbarten Funktionen auswirken können, und ob die zuständige Aufsichtsbehörde weiterhin in der Lage ist, das Finanzunternehmen angemessen zu beaufsichtigen (Art. 29 Abs. 2 DORA). Dass Bestandteil der Risikoevaluierung auch die Frage sein sollte, ob der betreffende IKT-Drittdienstleister zur Erbringung der avisierten Leistung grundsätzlich geeignet und zuverlässig ist und keine Interessenkonflikte bestehen, versteht sich von selbst (Art. 28 Abs. 4 lit. e) DORA).

b) Einhaltung von IT-Sicherheitsstandards

Vertragliche Bindungen dürfen nur mit IKT-Drittdienstleistern eingegangen werden, die angemessene IT-Standards, insbesondere in Bezug auf kritische oder wichtige Funktionen, gewährleisten (Art. 28 Abs. 5 DORA). Auch diese Anforderungen sind vorab zu evaluieren. Den jeweiligen Finanzunternehmen sind Zugangs-, Inspektions- und Auditrechte beim IKT-Drittdienstleister zu gewähren. Einzelheiten sind unter Berücksichtigung allgemein anerkannter Auditstandards vorab zu regeln (Art. 28 Abs. 6 DORA). Sofern vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen werden, ein hohes Maß an technischer Komplexität mit sich bringen, ist ferner zu prüfen und zu bewerten, inwieweit interne und externe Revisoren oder ein Revisorenpool über Fähigkeiten und Kenntnisse verfügen, die für die wirksame Durchführung der einschlägigen Audits und Bewertungen erforderlich sind.

c) Gesteigerte Anforderungen für sog. Kritische IKT-Drittdienstleister

Gemäß Art. 31 Abs. 1 lit. (a) DORA sind die zuständigen Europäischen Aufsichtsbehörden (European Supervisory Authorities – kurz ESA) berechtigt, IKT-Drittdienstleister nach bestimmten Kriterien als „kritisch" einzustufen. Solche Kriterien sind etwa (i) zu erwartende systemische Auswirkungen auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen im Falle einer Betriebsstörung aufseiten des IKT-Drittdienstleisters, (ii) der systemische Charakter oder die Bedeutung der Finanzunternehmen, die auf den jeweiligen IKT-Drittdienstleister zurückgreifen oder (iii) die Abhängigkeit von Finanzunternehmen von den Leistungen des betreffenden IKT-Drittdienstleisters (Art. 31 Abs. 2 DORA). Bislang haben die ESA eine Liste kritischer IKT-Drittdienstleister nicht veröffentlicht. Dies dürfte jedoch nur eine Frage der Zeit sein. Auf die weiteren Einzelheiten des Einstufungsverfahrens und in diesem Zusammenhang zu berücksichtigende Ausnahmekriterien vorliegend näher einzugehen, würde den Rahmen dieser Darstellung sprengen. Insoweit sei daher auf Art. 31 DORA verwiesen. IKT-Drittdienstleister, die von den ESA nicht als kritisch eingestuft worden sind, haben die Möglichkeit, ihre Einstufung als kritischer IKT-Drittdienstleister zu beantragen (Art. 31 Abs. 11 DORA).

4. Vertragliche Mindestanforderungen

Verträge mit IKT-Drittdienstleistern müssen bestimmten Mindestanforderungen an Regelungsinhalt und Regelungstiefe entsprechen (Art. 30 DORA). Hierbei sollen auch von den zuständigen Aufsichtsbehörden noch zu entwickelnde Standardvertragsklauseln Berücksichtigung finden (Art. 30 Abs. 4 DORA).[22] Die in Art. 30 DORA genannten und nachstehend näher erläuterten Anforderungen gelten auch für Altverträge. Diese sind von den Finanzunternehmen mit ihren jeweiligen IKT-Drittdienstleistern im Einklang mit den Anforderungen von DORA nachzuverhandeln und über entsprechende Änderungsverträge auf die Anforderungen von DORA nachzuziehen.[23] Hierzu sollen die zuständigen Behörden den Finanzunternehmen angemessene Umsetzungsspielräume gewähren, um nachteilige Auswirkungen auf ihre digitale operationale Resilienz zu vermeiden und ihnen die Anwendung der in Artikel 28 DORA genannten Ausstiegsstrategien und Übergangspläne zu ermöglichen, bevor behördliche Maßnahmen verhängt werden (Art. 42 Abs. 8 lit. f) DORA).

---

20 Siehe hierzu III.
21 Siehe unter I. 2).
22 ErwG 75 zu DORA.
23 ErwG 69 zu DORA.

a) Allgemeine Anforderungen

Dass Verträge mit IKT-Drittdienstleistern hinsichtlich ihrer Regelungsinhalte, insbesondere der von dem IKT-Drittdienstleister zu erbringenden Leistungen einschließlich deren Qualität vollständig, klar und unmissverständlich sein sollten, versteht sich von selbst, ebenso dass der betreffende Vertrag schriftlich und auf einem ihn dauerhaft verkörpernden Medium abzuschließen ist (Art. 30 Abs. 1 DORA). Als weitere vertragliche Inhalte sind gemäß Art. 30 Abs. 2 DORA in den Vertrag mit dem IKT-Drittdienstleister u. a. die folgenden Regelungen aufzunehmen:

- Eine klare und vollständige Beschreibung sämtlicher Funktionen und Leistungen, die der IKT-Drittdienstleister bereitzustellen hat, unter klarer Festlegung der Zulässigkeit und, im Falle einer solchen, der einzelnen Bedingungen der Vergabe von Unteraufträgen (Art. 30 Abs. 2 lit. (a) DORA);
- die Standorte – das heißt die Regionen und Länder –, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen bereitzustellen sind und an denen Daten verarbeitet werden sollen, einschließlich des Speicherorts, sowie die Auflage für den IKT-Drittdienstleister, das Finanzunternehmen vorab zu benachrichtigen, wenn eine Änderung eines oder mehrerer Standorte beabsichtigt ist Art. 30 Abs. 2 lit. (a) DORA);
- klare Regelungen zur Qualität der zu erbringenden Leistungen (Service Level), insbesondere deren Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit einschließlich des Schutzes personenbezogener Daten (Art. 30 Abs. 2 lit. (c) und (e) DORA);
- Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen benötigt werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format (Art. 30 Abs. 2 lit. (d) DORA);
- die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten Art. 30 Abs. 2 lit. (f) DORA);
- die Verpflichtung des IKT-Drittdienstleisters, vollumfänglich mit den zuständigen Behörden zusammenzuarbeiten, einschließlich der von diesen benannten Personen Art. 30 Abs. 2 lit. (g) DORA);
- Bedingungen für die Teilnahme des IKT-Drittdienstleisters an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz (Art. 13 Abs. 6 DORA); sowie
- Vereinbarungen zu Kündigungsrechten einschließlich geltender Kündigungsfristen entsprechend den Erwartungen der jeweils zuständigen Behörden (Art. 30 Abs. 2 lit. (h) DORA). In diesem Zusammenhang sind auch die in Art. 28 Abs. 7 DORA aufgeführten Kündigungsszenarien vertraglich abzubilden. Demnach soll dem Finanzunternehmen ein Kündigungsrecht insbesondere dann zustehen, wenn (i) der IKT-Drittdienstleister gegen geltendes Recht, sonstige Vorgaben oder vertragliche Bedingungen verstoßen hat, (ii) besondere Umstände vorliegen, die – allgemein formuliert – ein Risiko für die ordnungsgemäße Erbringung der vertraglich geschuldeten Leistungen oder Zweifel an der Verlässlichkeit des IKT-Drittdienstleisters aufkommen lassen, oder (iii) die zuständige Behörde das Finanzunternehmen infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr effektiv beaufsichtigen kann.

b) Besondere Anforderungen bei kritischen oder wichtigen Funktionen

Sind IKT-Leistungen zur Unterstützung kritischer oder wichtiger Funktionen Gegenstand des Vertrags mit dem IKT-Drittdienstleister, sind zusätzlich zu den unter Ziffer V.4.a) genannten Inhalten insbesondere die nachstehenden Mindestanforderungen vertraglich zu reflektieren:

- Eine vollständige Beschreibung der geltenden Leistungsqualitäten (Service Level), sowie deren Aktualisierung und Überarbeitung, einschließlich präziser quantitativer und qualitativer Leistungsziele pro Service Level (Art. 30 Abs. 3 lit. (a) DORA);
- Reportingverpflichtungen des IKT-Drittdienstleisters in inhaltlicher und zeitlicher Hinsicht, einschließlich der Verpflichtung, Entwicklungen zu melden, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters, IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus wie geschuldet bereitzustellen, auswirken könnten (Art. 30 Abs. 3 lit. (b) DORA);
- Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen sowie über Maßnahmen, Tools und Policies zur IKT-Sicherheit zu verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit den regulatorischen Bestimmungen bieten (Art. 30 Abs. 3 lit. (c) DORA);
- die Verpflichtung des IKT-Drittdienstleisters, sich an den in den Artikeln 26 und 27 genannten TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken (Art. 30 Abs. 3 lit. (d) DORA);
- uneingeschränkte Zugangs-, Kontroll- und Auditrechte des Finanzunternehmens selbst oder eines von ihm beauftragten Dritten sowie der zuständigen Aufsichtsbehörde einschließlich des Rechts zur Anfertigung von Kopien einschlägiger Unterlagen vor Ort, wobei die tatsächliche Ausübung dieser Rechte nicht durch andere vertragliche Vereinbarungen oder Umsetzungsrichtlinien behindert oder eingeschränkt wird (Art. 30 Abs. 3 lit. (e) (i) DORA), sowie alternativer Garantien für den Fall, dass Rechte anderer Kunden betroffen sein sollten (Art. 30 Abs. 3 lit. (e) (ii) DORA);
- die Verpflichtung des IKT-Drittdienstleisters zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits einschließlich der Verpflichtung, Einzelheiten zu Umfang und Häufigkeit solcher Maßnahmen mitzuteilen (Art. 30 Abs. 3 lit. (e) (iii) und (iv) DORA); sowie
- die Festlegung eines verbindlichen angemessenen Übergangszeitraums, in dem der IKT-Drittdienstleister die geschuldeten Leistungen auch über das Ende des Vertrages hinaus erbringt, um Störungen im Geschäftsbetrieb des Finanzunternehmens möglichst gering zu halten und dem Finanzunternehmen zu ermöglichen, den Vertrag geordnet abzuwickeln, zu einem Nachfolgedienstleister zu wechseln oder auf interne Lösungen umzustellen, die der Komplexität der erbrachten Leistungen entspricht.

Interessanterweise lässt der Katalog zwingender rechtlicher Regelungen in Art. 30 Abs. 3 DORA eine Verpflichtung zur Aufnahme vertraglicher Aussetzungs- und Kündigungsklauseln zugunsten des Finanzunternehmens für den Fall vermissen, dass die zuständige Aufsichtsbehörde von dem Finanzunternehmen die vorübergehende Aussetzung oder eine vollständige oder teilweise Beendigung der

Zusammenarbeit mit einem IKT-Drittdienstleister, der kritische oder wichtige Funktionen übernommen hat, verlangen sollte. Derartige Vertragsklauseln sind nicht nur unter Berücksichtigung in Deutschland geltender finanzregulatorischer Anforderungen zu empfehlen. Auch Art. 42 Abs. 6 DORA räumt den zuständigen Behörden bei Vorliegen bestimmter Risiken solche Möglichkeiten ein. Da unmittelbarer Adressat einer derartigen Regulierungsverfügung regelmäßig das der Regulierung unterstehende Finanzunternehmen, weniger der IKT-Drittdienstleister sein dürfte, sollte die Situation vermieden werden, dass das Finanzunternehmen in einem solchen Fall von einer vertraglichen Vereinbarung mit dem betreffenden IKT-Drittdienstleister nicht mehr oder nur noch unter erheblichen – insbesondere finanziellen – Nachteilen Abstand nehmen kann. Dem sollte im Wege angemessener vertraglicher Aussetzungs- und Loslösungsrechte dringend vorgebeugt werden.

VI. Fazit und Handlungsempfehlungen

DORA stellt für die Cybersicherheitsstrategie der EU einen elementaren Bestandteil dar und gibt als erstes europäisches branchenspezifisches Gesetz zur IT-Sicherheit wesentliche, sinnvolle Regelungen zur Schaffung eines einheitlich hohen Schutzniveaus für den Finanzsektor vor. DORA tritt bereits am 16.1.2023 in Kraft. Die Vorgaben sind bis zum 17.1.2025 von den Regelungsadressaten umzusetzen. Angesichts der Herausforderungen für Finanzunternehmen erscheint die Übergangsfrist also durchaus sportlich. Betroffenen Unternehmen ist daher anzuraten, bereits jetzt bestimmte Maßnahmen einzuleiten, um den knappen Zeitraum möglichst effizient zu nutzen.
Im Bereich des Governance- und Kontrollrahmens[24], des IKT-Risikomanagementrahmens[25] und der Prüfpflichten[26] sollten Finanzunternehmen mittels einer Gap-Analyse die neuen Vorgaben mit sämtlichen bereits vorhandenen Prozessen abgleichen, um so festzustellen, für welche Prozesse welcher spezifische Handlungsbedarf besteht. Das Gleiche gilt für das IKT-Drittdienstleistermanagement[27]. Neben einem Abgleich der bereits vorhandenen Prozesse zu Maßnahmen vor der Einbindung eines IKT-Drittdienstleisters mit den Vorgaben aus DORA sollten Finanzunternehmen sämtliche bestehenden IKT-Verträge im Hinblick auf Vertragsgegenstände, insbesondere deren kritische oder wichtige Funktionen prüfen. Sofern unter der Berücksichtigung der Vorgaben aus DORA Nachbesserungsbedarf besteht, sollten Nachverhandlungen mit Dienstleistern frühzeitig initiiert werden. Dies gilt insbesondere vor dem Hintergrund, dass sämtliche von DORA betroffenen Marktteilnehmer in den nächsten zwei Jahren mit einer überbordenden Anzahl an neuen Verhandlungen oder Nachverhandlungen mit sämtlichen ihrer Kunden, die als Finanzunternehmen gelten, verstärkt beschäftigt sein dürften.

AUTOREN

Dr. Thorsten Ammann
berät national und international operierende Unternehmen zu allen Belangen des Informationstechnologierechts mit besonderer Fokussierung auf Digitale Transformationsprojekte und Disruptive Technologien, insbesondere Blockchains, Künstlicher Intelligenz, IoT und Smart Factories. Dr. Thorsten Ammann ist Co-Autor diverser juristischer Standardwerke, u. a. des Computerrechtshandbuchs und des Rechtshandbuchs Artificial Intelligence und Machine Learning.

Yannick Zirnstein
berät national und international operierende Unternehmen zu allen Aspekten des deutschen und europäischen Rechts in den Bereichen Informationstechnologie, Cybersecurity und Datenschutz. Yannick Zirnstein ist Autor diverser Publikationen, u. a. im Bereich Cybersecurity und Datenschutz.

24 Abschnitt IV.1.
25 Abschnitt IV.2.
26 Abschnitt IV.3.
27 Abschnitt V.