# Countdown DORA: 15 Kernpunkte der Verordnung über die digitale operationale Resilienz im Finanzsektor

27. November 2023

*Mit der Verordnung über die Digitale Operationale Resilienz im Finanzsektor („Digital Operational Resilience Act („DORA")" - Verordnung (EU) 2022/2554 – (hier abrufbar)) hat die EU einen Rechtsrahmen geschaffen, der die Stabilität, Sicherheit und Widerstandsfähigkeit digitaler Dienste stärken soll, um Verbraucher und den Finanzsektor vor Cyber-Bedrohungen zu schützen. DORA gilt für Finanzinstitute aber auch für Unternehmen, die IT-Leistungen an diese erbringen, insbesondere Cloud-Anbieter. Diese Unternehmen müssen dafür Sorge tragen, die Anforderungen von DORA spätestens bis zum Januar 2025 umzusetzen, um den in DORA vorgesehenen Sanktionen zu entgehen. Dazu gehören insbesondere die Aufrechterhaltung einer wirksamen Verteidigung gegen Cyberbedrohungen, die Einrichtung von Mechanismen zur Reaktion auf Sicherheitsvorfälle und die Sicherstellung von Geschäftskontinuität. Im Folgenden werden 15 Kernpunkte von DORA dargestellt, um Unternehmen einen Überblick darüber zu verschaffen, ob DORA auf sie anwendbar ist, welche Anforderungen sie stellt und was bei der Umsetzung zu beachten ist.*

1. **Ab wann gilt DORA?**
   DORA trat am 16. Januar 2023 in Kraft und wird ab dem 17. Januar 2025 uneingeschränkt zur Anwendung kommen.

2. **Was ist das Ziel der DORA?**
   Primäres Ziel ist es, mit DORA die digitale Betriebsstabilität und IT-Sicherheit von Finanzunternehmen vor schwerwiegenden Störungen, die im Zusammenhang mit Informations- und Kommunikationstechnologien („IKT") auftreten können, zu schützen und deren Geschäftskontinuität EU-übergreifend laufend aufrechtzuerhalten. Insbesondere sollen Finanzunternehmen durch die Umsetzung der DORA in die Lage versetzt werden, Cyberangriffe abzuwehren, strukturelle Risiken, die sich etwa aus der Konzentration der IKT in den Händen weniger Drittanbieter ergeben, abzumildern, sowie technische Komplikationen, die die Betriebsstabilität beeinträchtigen können, zu behandeln.

3. **Auf welche Unternehmen ist DORA anwendbar?**
   DORA ist auf im EU-Finanz- und Versicherungssektor tätige Unternehmen und Institutionen aus insgesamt zwanzig, in Art. 2 Abs. 1 lit. a)-t) DORA aufgeführten, Tätigkeitsbereichen (sog. „Finanzunternehmen") anwendbar. Hierzu zählen (a) Kreditinstitute, (b) Zahlungsinstitute, einschließlich gemäß der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute, (c) Kontoinformationsdienstleister, (d) E-Geld-Institute, einschließlich gemäß der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute, (e) Wertpapierfirmen, (f) Anbieter von Krypto-Dienstleistungen, die gemäß der sogenannten „Verordnung über Märkte von Krypto-Werten" zugelassen sind, und Emittenten wertreferenzierter Token, (g) Zentralverwahrer, (h) zentrale Gegenparteien, (i) Handelsplätze, (j) Transaktionsregister, (k) Verwalter alternativer Investmentfonds, (l) Verwaltungsgesellschaften, (m) Datenbereitstellungsdienste, (n) Versicherungs- und Rückversicherungsunternehmen, (o) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, (p) Einrichtungen der betrieblichen Altersversorgung, (q) Ratingagenturen, (r) Administratoren kritischer Referenzwerte, (s) Schwarmfinanzierungsdienstleister und (t) Verbriefungsregister.

Darüber hinaus erstreckt sich der Anwendungsbereich der DORA gem. Art. 2 Abs. 1 lit. u) auch auf Unternehmen, die zwar selbst keine Finanzunternehmen sind, aber IT-Leistungen an diese erbringen (sog. „IKT-Drittdienstleister"), wie etwa Cloud-Anbieter. Eine Vielzahl der DORA-Regelungen sind allerdings auf Kleinstunternehmen (d.h. Finanzunternehmen, die weniger als zehn Personen beschäftigen und deren Jahresumsatz bzw. -bilanzsumme EUR 2 Mio. nicht überschreitet) nicht oder nur in eingeschränkter Weise anwendbar.

**4. Was sind die wesentlichen Regelungen der DORA?**

Die wesentlichen DORA-Regelungen sind in den Kapiteln II-VII DORA enthalten und betreffen die Pflicht zur Errichtung und Aufrechterhaltung eines effektiven IKT-Risikomanagements (Kapitel II DORA); die effektive Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kapitel III DORA); das regelmäßige Testen der digitalen operationalen Resilienz (Kapitel IV DORA); das Management des IKT-Drittparteienrisikos (Kapitel V Abschnitt I DORA); die aufsichtliche Überwachung und Sanktionierung kritischer IKT-Drittdienstleister (Kapitel V Abschnitt II DORA); sowie die aufsichtliche Überwachung und Sanktionierung von Finanzunternehmen (Kapitel VII DORA).

**5. Welche Anforderungen stellt DORA an das IKT-Risikomanagement?**

Finanzunternehmen trifft die Pflicht zur Etablierung und jährlichen (für Kleinstunternehmen „regelmäßigen") Überprüfung und Dokumentation eines umfassenden, internen Governance- und Kontrollrahmens, um IKT-Risiken wirksam begegnen zu können. Was im Einzelnen im Rahmen des IKT-Risikomanagements umzusetzen ist, ist in Art. 5 Abs. 2 DORA beschrieben. Die Definition, Genehmigung, Überwachung und Verantwortung für die Umsetzung des IKT-Risikomanagements obliegt dem Leitungsorgan des Finanzunternehmens. Finanzunternehmen, die keine Kleinstunternehmen sind, müssen zudem eine unabhängige Kontrollfunktion hinsichtlich des IKT-Risikomanagements etablieren.

**6. Wie ist mit IKT-bezogenen Vorfällen umzugehen?**

Finanzunternehmen müssen Verfahren und Prozesse festlegen, nach denen IKT-bezogene Vorfälle möglichst frühzeitig erkannt, behandelt und gemeldet werden. Schwerwiegende IKT-bezogene Vorfälle sind verpflichtend der jeweils zuständigen Aufsichtsbehörde mittels eines 3-stufigen Meldeverfahrens zu melden. Auch müssen Finanzunternehmen ihre Kunden unverzüglich nach Kenntniserlangung über den schwerwiegenden IKT-bezogenen Vorfall benachrichtigen, wenn dieser Auswirkungen auf die finanziellen Interessen der Kunden hat. Erhebliche Cyberbedrohungen sind von den Finanzunternehmen ebenfalls zu erfassen, wobei eine Meldung diesbezüglich freiwillig erfolgen kann.

**7. Welche Anforderungen bestehen hinsichtlich der Testung der digitalen operationalen Resilienz?**

Finanzunternehmen, die keine Kleinstunternehmen sind, müssen ein solides und umfassendes Testprogramm etablieren, um ihre Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten, Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmaßnahmen umgehend umzusetzen. Die Tests sind von unabhängigen internen oder externen Parteien durchzuführen und sollen bei IKT-Systemen oder -anwendungen, die kritische oder wichtige Funktionen unterstützen, mindestens einmal jährlich stattfinden. Eine Auswahl an in Betracht kommenden Tests ist in Art. 25 Abs. 1 DORA genannt. Von bestimmten Finanzunternehmen wird nach Art. 26 DORA zusätzlich verlangt, dass diese mindestens im 3-Jahres-Zyklus sogenannte TLPT-Tests durchführen.

8. **Welche Anforderungen stellt DORA an das Management des IKT-Drittparteienrisikos und die vertraglichen Vereinbarungen mit IKT-Drittdienstleistern?**
Zur wirksamen Steuerung des IKT-Drittparteienrisikos haben Finanzunternehmen gemäß Art 28 Abs. 3 DORA ein stets aktuelles Informationsregister zu führen, das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleistern bereitgestellten IKT-Dienstleistungen bezieht. Vor Abschluss einer vertraglichen Vereinbarung mit einem IKT-Drittdienstleister müssen Finanzunternehmen zudem eine Risikoanalyse hinsichtlich des IKT-Drittdienstleisters anhand der in Art. 28 Abs. 4 und Abs. 5 DORA genannten Kriterien durchführen. Im Rahmen der Vertragsverhandlungen mit IKT-Drittdienstleistern haben die Finanzunternehmen sicherzustellen, dass die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche vorab bestimmt werden. Zudem ist vertraglich sicherzustellen, dass dem Finanzunternehmen Kündigungsrechte für die in Art. 28 Abs. 7 DORA genannten Fälle eingeräumt werden und im Falle von kritischen oder wichtigen Funktionen für den Beendigungsfall der Vertragsbeziehung angemessene Ausstiegsstrategien vorgesehen sind. Schließlich sieht Art. 30 DORA weitere wesentliche Vertragsbestimmungen vor, die im Rahmen der vertraglichen Vereinbarungen zwischen Finanzunternehmen und IKT-Drittdienstleistern zu beachten sind.

9. **Wie und von wem werden IKT-Drittdienstleister unter der DORA überwacht?**
Die europäischen Aufsichtsbehörden EBA, ESMA und EIOPA (sog. „ESA") überprüfen IKT-Drittdienstleister anhand konkreter, in Art. 31 Abs. 2 DORA genannter Kriterien und stufen diese ggf. als „kritisch" ein. Für jeden kritischen IKT-Drittdienstleister wird eine der ESA zur „federführenden Überwachungsbehörde" ernannt. Zu den Befugnissen der federführenden Überwachungsbehörde nach Art. 35 Abs. 1 DORA gehören u.a. (a) das Recht zur Anforderung aller einschlägiger Informationen und Unterlagen die sie zu ihrer Aufgabenerfüllung als notwendig erachtet, (b) die Durchführung allgemeiner Untersuchungen und (Vor-Ort-)Inspektionen, (c) die Anforderung von Berichten nach Abschluss der Überwachungstätigkeiten, sowie (d) das Aussprechen von Empfehlungen, etwa in Bezug auf IKT-Sicherheits- und Qualitätsanforderungen oder zur Unterauftragsvergabe.

10. **Welche Sanktionen sieht DORA gegen IKT-Drittdienstleister im Falle von Verstößen vor?**
Zur Durchsetzung ihrer Befugnisse nach Art. 35 Abs. 1 (a)-(c) DORA kann die federführende Überwachungsbehörde ein verwaltungsrechtliches Zwangsgeld in Höhe von bis zu 1% des durchschnittlichen weltweiten Tagesumsatzes, den der kritische IKT-Drittdienstleister im vorangegangenen Geschäftsjahr erzielt hat, verhängen. Das Zwangsgeld wird täglich bis zur Einhaltung der Vorschriften, jedoch höchstens für sechs Monate verhängt. Verhängte Zwangsgelder werden von der federführenden Überwachungsbehörde grds. veröffentlicht. Hinsichtlich einer Empfehlung nach Art. 35 Abs. 1 (d) DORA sind kritische IKT-Drittdienstleister dazu verpflichtet, der federführenden Überwachungsbehörde innerhalb von 60 Kalendertagen mitzuteilen, ob sie beabsichtigen, dieser Empfehlung Folge zu leisten, oder eine begründete Erklärung für die Nichtbefolgung der Empfehlungen vorzulegen. Die federführende Überwachungsbehörde informiert öffentlich darüber, wenn ein kritischer IKT-Drittdienstleister es versäumt, die federführende Überwachungsbehörde entsprechend der DORA Anforderungen zu unterrichten, oder wenn die Erklärung des kritischen IKT-Drittdienstleisters als nicht ausreichend erachtet wird. Darüber hinaus unterrichten in einem solchen Fall auch die zuständigen nationalen Behörden die betreffenden Finanzunternehmen und können von diesen vorübergehend die teilweise oder vollständige Einstellung des Einsatzes des jeweiligen IKT-Drittdienstleisters oder die teilweise oder vollständige Kündigung des einschlägigen Vertragsverhältnisses verlangen.

11. **Wie und von wem werden Finanzunternehmen unter der DORA überwacht?**
Die behördliche Zuständigkeit für das jeweilige Finanzunternehmen folgt aus Art. 46 DORA. Die zuständigen Behörden verfügen über alle Aufsichts-, Untersuchungs- und Sanktionsbefugnisse, die zur

Erfüllung ihrer Aufgaben im Rahmen der DORA erforderlich sind. Die Befugnisse umfassen gem. Art. 50 Abs. 2 DORA zumindest (a) den Zugriff auf Unterlagen oder Daten jeglicher Form, die nach Ansicht der zuständigen Behörde für die Ausführung ihrer Aufgaben von Belang sind, sowie den Erhalt oder Anfertigung von Kopien von ihnen, (b) die Durchführung von Vor-Ort-Inspektionen oder Untersuchungen, und (c) das Verlangen von Korrektur- und Abhilfemaßnahmen bei Verstößen gegen die Anforderungen der DORA.

**12. Welche Sanktionen sieht DORA gegen Finanzunternehmen im Falle von Verstößen vor?**

Die EU-Mitgliedsstaaten haben nach Art. 50 Abs. 3 DORA angemessene verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen für Verstöße gegen die DORA festzulegen und für deren wirksame Umsetzung zu sorgen. Diese Sanktionen und Maßnahmen müssen wirksam, verhältnismäßig und abschreckend sein. Verwaltungsrechtliche Sanktionen werden nach Art. 54 DORA durch die zuständige Behörde auf ihren amtlichen Websites unverzüglich veröffentlicht. Zwar legt DORA keine strafrechtlichen Sanktionen für Verstöße fest, den EU-Mitgliedstaaten steht es jedoch frei, solche in ihrem nationalen Recht vorzusehen.

**13. Inwieweit weichen die DORA-Regelungen von den in Deutschland bereits geltenden Regularien ab?**

Die DORA-Regelungen sind mit den für den deutschen Finanz- und Versicherungssektor bereits geltenden nationalen und europäischen Regularien für das Risikomanagement von Cyber- und IT-Risiken, insbesondere der MaRisk, BAIT, ZAIT, KAMaRisk/KAIT sowie den EBA- und ESMA-Leitlinien zur Auslagerung an Cloud-Anbieter, inhaltlich zwar weitgehend kongruent. Dennoch gehen die DORA-Regelungen teilweise präziser ins Detail oder weichen von den derzeit geltenden Regularien ab. So ist beispielsweise gemäß DORA eine neue unabhängige Kontrollfunktion für das Management und die Überwachung des IKT-Risikos einzurichten. Auch werden die Anforderungen an Tests präzisiert und durch die Forderung von erweiterten Tests auf Grundlage von TLPT verschärft. Für manche Finanzunternehmen, z.B. Kapitalverwaltungsgesellschaften, ist auch das Meldewesen für Sicherheitsvorfälle neu. Zudem ist der Anwendungsbereich der DORA wesentlich umfangreicher als die für den deutschen Finanz- und Versicherungssektor derzeit geltenden Regularien, da DORA auf mehr Unternehmen (insb. IKT-Drittdienstleister) unmittelbar Anwendung findet und nicht zwischen Auslagerung und sonstigem Fremdbezug differenziert. Schließlich ist hervorzuheben, dass DORA, anders als die bislang geltenden Regularien, die Gesamtverantwortung für Nichteinhaltung der DORA explizit dem Leitungsorgan der Finanzunternehmen zuordnet, welches seine Kenntnisse und Fähigkeiten in Bezug auf IKT-Risiken aktiv auf dem neuesten Stand zu halten und an regelmäßigen IKT-bezogenen Schulungen teilzunehmen hat, um die IKT-Risiken und deren Auswirkungen verstehen und bewerten zu können.

**14. Wie verhält sich DORA zu bereits bestehenden Regularien sowie zur NIS-2-Richtlinie?**

Im Verhältnis zu den bereits bestehenden Regularien auf EU-Ebene sowie der am 27. Dezember 2022 veröffentlichten und bis zum 27. Oktober 2024 ins nationale Recht umzusetzenden NIS-2-Richtlinie ist DORA gemäß ihres Erwägungsgrunds 16 als lex specialis zu betrachten.

Neben DORA wurde zeitgleich eine DORA-Änderungsrichtlinie mit dem Ziel veröffentlicht, sektorale europäische Richtlinien konsistent mit den Anforderungen von DORA zu halten. So wurden beispielsweise TLPT unter DORA in den SREP-Prozess der Eigenkapitalrichtlinie (Capital Requirements Directive – CRD) aufgenommen. Die DORA-Änderungsrichtlinie ändert die europäischen Richtlinien 2009/65/EG (OGAW-Richtlinie), 2009/138/EG (Solvency II), 2011/61/EU (AIFM-Richtlinie), 2013/36/EU

(Eigenkapitalrichtlinie; CRD), 2014/59/EU (Abwicklungsrichtlinie), 2014/65/EU (MiFID II), (EU) 2015/2366 (PSD II) und (EU) 2016/2341 (EbAV-II-Richtlinie).

**15. Was sollten betroffene Unternehmen tun, um die Anforderungen der DORA effektiv umzusetzen?**

Finanzunternehmen und IKT-Drittdienstleister sollten bereits jetzt mit einer GAP-Analyse beginnen und die identifizierten Lücken schnellstmöglich, spätestens bis zum Januar 2025, schließen. Aufgrund der weitgehenden Kongruenz mit den bereits bestehenden nationalen und europäischen Regularien für den Finanz- und Versicherungssektor, bietet sich für die Umsetzung der DORA eine Orientierung an diesen an. Als zusätzliche Orientierungshilfe wird die ESA gemäß ihrer Pflicht nach Art. 28 Abs. 10 DORA bis zum 17. Januar 2024 zu einigen Themen Spezifikationen in Form von technischen Regulierungsstandards (RTS) und technischen Durchführungsstandards (ITS) an die EU-Kommission übermitteln. Vier dieser Spezifikationen wurden bereits am 19. Juni 2023 zur öffentlichen Konsultation bis zum 11. September 2023 veröffentlicht (hier abrufbar). Die Veröffentlichung weiterer Spezifikationen zur öffentlichen Konsultation wird bis Anfang Dezember 2023 erwartet.

**Ihre Kontakte bei YPOG:**

**Dr. Lutz Schreiber**
Partner, Hamburg
IP/IT/Data Protection

+49 406077281 234
+49 151 40229483
lutz.schreiber@ypog.law

**Sara Apenburg**
Senior Associate, Hamburg
IP/IT/Data Protection

+49 40 6077281 237
+49 151 40229489
sara.apenburg@ypog.law