YPOG Briefing

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

12. September 2024

*Mit der Verordnung über die Digitale Operationale Resilienz im Finanzsektor („Digital Operational Resilience Act („DORA")" - Verordnung (EU) 2022/2554 – (abrufbar **hier**)) 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 und welche weiteren Regelungen wurden im Zusammenhang mit DORA veröffentlicht?**

   DORA trat am 16. Januar 2023 in Kraft und wird ab dem 17. Januar 2025 uneingeschränkt zur Anwendung kommen. Als zusätzliche Orientierungshilfe zur Implementierung und Umsetzung von DORA haben die europäischen Aufsichtsbehörden EBA, ESMA und EIOPA (zusammen die „ESA") ergänzende Standards veröffentlicht, die Spezifikationen zu bestimmten Themen in Form von technischen Regulierungsstandards (RTS), technischen Durchführungsstandards (ITS) und Leitlinien enthalten. Des Weiteren hat die Europäische Kommission Spezifizierungen im Rahmen von delegierten Rechtsakten erlassen. Eine Übersicht der veröffentlichten RTS, ITS, Leitlinien und delegierten Rechtsakte ist **hier** abrufbar. 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 Threat Led Penetration Tests („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).

2. **Was ist das Ziel von 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 von 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 aufgeführte, 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 gem. Art. 2 Abs. 1 lit. (u) DORA 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 2 Mio. EUR nicht überschreitet) nicht oder nur in eingeschränkter Weise anwendbar.

Hingegen sind die folgenden, in Art. 2 Abs. 3 DORA genannten Unternehmen, von DORA nicht erfasst: (a) Verwalter alternativer Investmentfonds im Sinne von Art. 3 Abs. 2 der Richtlinie 2011/61/EU, (b) Versicherungs- und Rückversicherungsunternehmen im Sinne von Art. 4 der Richtlinie 2009/138/EG, (c) Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 15 Versorgungsanwärtern betreiben, (d) gemäß den Artikeln 2 und 3 der Richtlinie 2014/65/EU ausgenommene natürliche oder juristische Personen, (e) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt, sowie (f) Postgiroämter im Sinne von Art. 2 Abs. 5 Nr. 3 der Richtlinie 2013/36/EU.

4. Was sind die wesentlichen Regelungen von 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 Kompetenzen und Pflichten der zuständigen Behörden (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 für die Überwachung und das Management von IKT-Risiken einrichten. Zur Spezifizierung der Anforderungen an die Einrichtung eines IKT-Risikomanagements haben die ESA die „RTS zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens" veröffentlicht (abrufbar **hier**).

6. Wie ist mit IKT-bezogenen Vorfällen umzugehen?

Finanzunternehmen müssen Verfahren und Prozesse festlegen, nach denen IKT-bezogene Vorfälle möglichst frühzeitig erkannt, behandelt, klassifiziert und gemeldet werden. IKT-bezogene Vorfälle, die gemäß den Kriterien in Art. 18 Abs. 1 DORA als schwerwiegend zu klassifizieren sind, sind verpflichtend der jeweils zuständigen Aufsichtsbehörde mittels eines dreistufigen 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. Cyberbedrohungen, die gemäß den Kriterien in Art. 18 Abs. 2 DORA als erheblich zu klassifizieren sind, sind von den Finanzunternehmen ebenfalls zu erfassen, wobei eine Meldung diesbezüglich freiwillig erfolgen kann. Zur Identifizierung solcher Vorfälle haben die ESA die „RTS zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle" veröffentlicht (abrufbar **hier**). Spezifizierungen hinsichtlich der Meldung solcher Vorfälle sind in den von den ESA veröffentlichten „RTS zur Festlegung des Inhalts der Meldung schwerwiegender IKT-Vorfälle und erheblicher Cyberbedrohungen sowie zur Bestimmung der Fristen der Meldung von schwerwiegenden Vorfällen" (abrufbar **hier**) und den „ITS zur Festlegung von Standardformularen, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung" (abrufbar **hier**) enthalten.

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 alle drei Jahre Threat Led Penetration Tests („TLPT") durchführen. Die Anforderungen an diese Tests wurden von den ESA in den „RTS zur Speziierung von Elementen im Zusammenhang mit Threat Led Penetration Tests" spezifiziert (abrufbar **hier**).

8. Welche Anforderungen stellt DORA an das Management des IKT-Drittparteienrisikos und die vertraglichen Vereinbarungen mit IKT-Drittdienstleistern?

Mit Ausnahme von Kleinstunternehmen haben IKT-Drittdienstleister die Pflicht zur Erstellung und regelmäßigen Überprüfung einer Strategie zum IKT-Drittparteienrisiko sowie einer Leitlinie für die Nutzung von IKT-Drittdienstleistungen. Diesbezüglich haben die ESA die „RTS 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" veröffentlicht (abrufbar **hier**). Zur wirksamen Steuerung des IKT-Drittparteienrisikos haben Finanzunternehmen gemäß Art. 28 Abs. 3 DORA ein stets aktuelles Informationsregister zu führen. Konkretisierungen hierzu finden sich in den von den ESA veröffentlichten „ITS zur Erstellung einer Standardvorlage für das

Informationsregister" (abrufbar **hier**). Das Informationsregister soll aktuelle Informationen über alle ausgelagerten IKT-Prozesse, die entsprechenden vertraglichen Vereinbarungen und die Einordnung als kritische/wichtige oder nichtkritische/nichtwichtige Funktion beinhaltet und ist den zuständigen Behörden auf Verlangen ganz oder, sofern angefragt, teilweise zur Verfügung zu stellen. Zudem haben Finanzunternehmen den zuständigen Behörden mindestens einmal jährlich Bericht zu erstatten zur Anzahl neuer Vereinbarungen über die Nutzung von IKT-Dienstleistungen, den Kategorien von IKT-Drittdienstleistern, der Art der vertraglichen Vereinbarungen sowie den bereitgestellten IKT-Dienstleistungen und -Funktionen. Finanzunternehmen haben die zuständigen Behörden ferner zeitnah 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 benachrichtigen.

Vor Abschluss einer vertraglichen Vereinbarung mit einem IKT-Drittdienstleister müssen Finanzunternehmen 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, unter anderem bezüglich der Zulässigkeit und der Bedingungen für die Unterauftragsvergabe. Hierzu haben die ESA die „RTS zur Festlegung der Elemente, die ein Finanzunternehmen bei der Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, bestimmen und bewerten muss" veröffentlicht (abrufbar **hier**).

9. Wie und von wem werden IKT-Drittdienstleister unter DORA überwacht?

Die ESA überprüfen IKT-Drittdienstleister anhand konkreter, in Art. 31 Abs. 2 DORA genannter Kriterien und stufen diese ggf. als „kritisch" ein. Zur Spezifizierung der hierfür heranzuziehenden Kriterien hat die Europäische Kommission die „Delegierte Verordnung zu den Kriterien zur Festlegung der Kriterien für die Einstufung von IKT-Drittdienstleistern als für Finanzunternehmen kritisch" veröffentlicht (abrufbar **hier**). 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 gegen kritische IKT-Drittdienstleister 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 lit. (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 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 von 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 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 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, VAIT, KAMaRisk, KAIT sowie den EBA- und ESMA-Leitlinien zur Auslagerung an Cloud-Anbieter, inhaltlich 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 das Testen der digitalen operationalen Resilienz präzisiert und durch die Forderung von erweiterten Tests auf Grundlage von TLPT verschärft. Daneben gehen DORA-Anforderungen bezüglich der Inhalte der Verträge mit IKT-Drittdienstleistern an einigen Stellen über die Anforderungen der derzeit geltenden Regelungen hinaus. Für manche Finanzunternehmen, z.B. Kapitalverwaltungsgesellschaften, ist auch das Meldewesen für Sicherheitsvorfälle neu. Zudem ist der Anwendungsbereich von 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 die Nichteinhaltung von 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 und somit als vorrangig zu betrachten. In Bereichen, in denen die Regelungen der NIS-2 spezifischer sind als die von DORA, gelten die NIS-2 Vorschriften jedoch ergänzend. Nationale Regularien und Anforderungsvorgaben, etwa die BAIT, sind so anzupassen, dass sie mit den DORA-Anforderungen konsistent sind, wobei spezifische nationale Besonderheiten bestehen bleiben können.

15. **Was sollten betroffene Unternehmen tun, um die Anforderungen der DORA effektiv umzusetzen?**
    Finanzunternehmen und IKT-Drittdienstleister sollten eine GAP-Analyse hinsichtlich ihrer existierenden Prozesse, internen Dokumentationen und Verträge mit IKT-Drittdienstleistern erstellen. Die identifizierten Lücken sollten durch Implementierung der im Rahmen der Gap Analyse als fehlend festgestellten internen Prozesse sowie durch den Entwurf neuer bzw. Anpassung vorhandener Richtlinien und Dokumentationen schnellstmöglich, spätestens bis zum Januar 2025, geschlossen werden. Zudem sind vorhandene Verträge zwischen Finanzunternehmen und IKT-Drittdienstleistern nachzuverhandeln und zu aktualisieren, sodass diese die DORA-Anforderungen angemessen reflektieren. Insbesondere die IKT-Drittdienstleister sollten hierfür Anpassungen an ihren Standardverträgen vornehmen und DORA-Zusatzvereinbarungen vorbereiten, die sie Finanzunternehmen als Zusatz zu ihren Vertragsunterlagen anbieten können, um Ihnen die Einhaltung der DORA-Anforderungen in Bezug auf vertragliche Vereinbarungen mit IKT-Drittdienstleistern zu ermöglichen. Neben den DORA-Anforderungen selbst, sollten Finanzunternehmen und IKT-Drittdienstleister insbesondere die Spezifizierungen der ESA in Form der RTS, ITS und Leitlinien berücksichtigen, da diese praktische Anleitungen zur Umsetzung der DORA-Anforderungen enthalten. Weitere Hilfestellungen bietet die deutsche Aufsichtsbehörde BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) in ihren Aufsichtsmitteilungen zu DORA und sonstigen Beiträgen, die auf der Website der BaFin zu finden sind (abrufbar **hier**).

Fazit: Die Umsetzung der DORA-Anforderungen stellt eine Herausforderung für viele Finanzunternehmen und in der Finanzbranche tätige IT-Dienstleister dar, die es schnellstmöglich zu bewältigen gilt. Gerne unterstützen wir Sie zu rechtlichen Fragen rund um dieses Thema.

Ihre Kontakte bei YPOG:

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

+49 406077281 234
+49 151 40229483

Sara Apenburg
Partner, Hamburg
IP/IT/Data Protection

+49 40 6077281 237
+49 151 40229489

lutz.schreiber@ypog.law sara.apenburg@ypog.law