TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-"IT-Sicherheitsrechtstag" 2024

Berlin, 25.09.2024

Der Digital Operational Resilience Act (DORA)

Rechtsanwalt Vincent Oppelland, Haufe Lexware

DORA als Teil des Digital Finance Package

Quelle: Europäische Kommission

DORA ist Teil des Digital Finance Package (2020)

- **Digital Operational Resilience Act (DORA): zielt darauf ab, die digitale betriebliche Widerstandsfähigkeit des Finanzsektors zu stärken.**
- Markets in Crypto-Assets Regulation (MiCAR): Rechtsakt über Märkte für Kryptowerte.
- Pilotregelung für DLT-basierte Marktinfrastrukturen: Vorschlag für auf Distributed-Ledger-Technologie basierende Marktinfrastrukturen.
- Retail Payments Strategy: Strategie für den Zahlungsverkehr.

DORA – Zweck und Anwendungsbereich

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

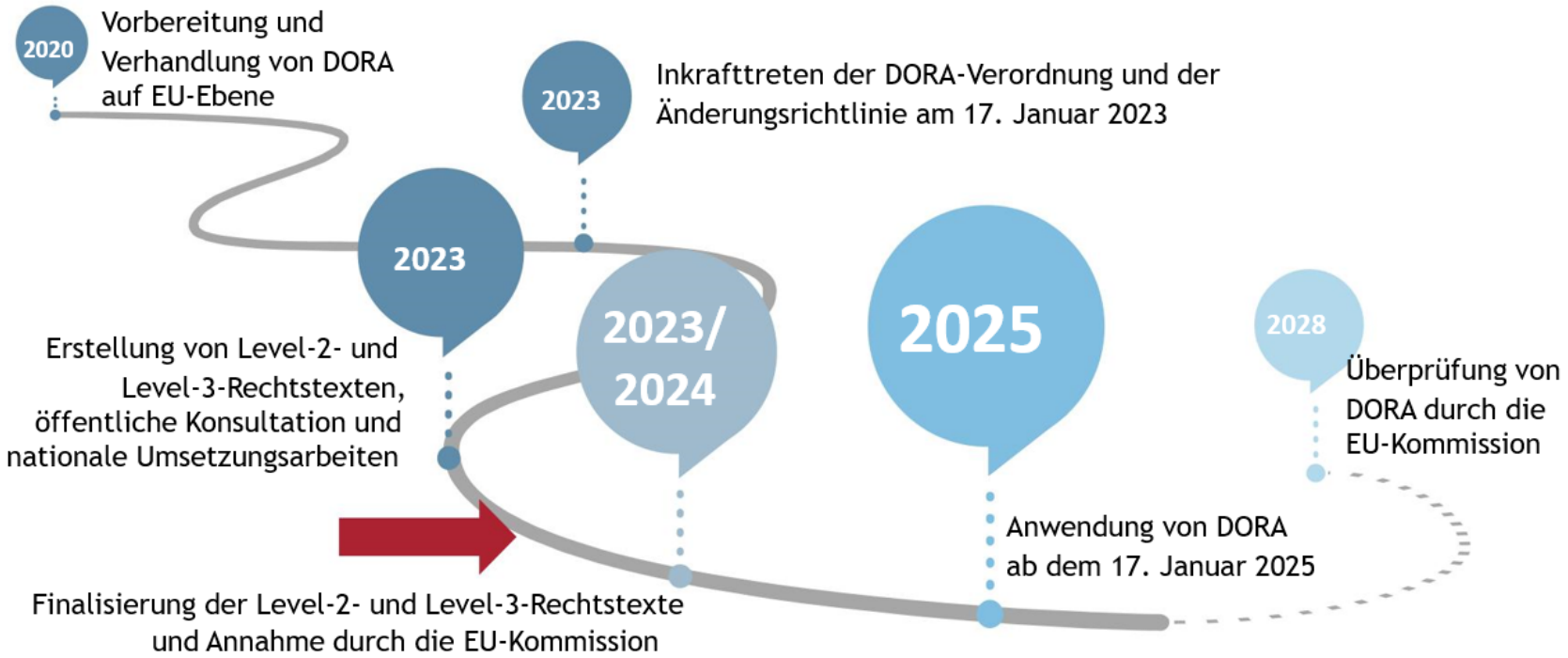
Was bezweckt DORA?

- Stärkung
  - Sicherheit und operationale Resilienz im europäischen Finanzsektor
- Harmonisierung
  - Einheitliche Anforderungen für den gesamten Finanzsektor
- Proportionalität
  - Anforderungen und Umsetzung müssen proportional sein (Art. 4 DORA)

Für wen gilt der DORA?

- Finanzunternehmen (Art. 2 Abs. 1 lit. a – t)
  - u.a. Banken, Versicherungen, Zahlungsinstitute
- IKT-Drittdienstleister (Art. 2 Abs.1 lit. u)

DORA - Timeline



Quelle: BaFin

DORA - Themenbereiche

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- IKT-Risikomanagement (Kapitel II, Artikel 5–16)
- Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kapitel III, Artikel 17-23)
- Testen der digitalen operationalen Resilienz, u.U. auch Threat-Led Penetration Testing (TLPT, Kapitel IV, Artikel 24-27)
- IKT-Drittparteienrisikomanagement (Kapitel V, Abschnitt I, Artikel 28-30)
- EU-Überwachungsrahmenwerk: Überwachung von kritischen IKT-Dienstleistern (Kapitel V, Abschnitt II, Artikel 31-44)
- Vereinbarungen über den Austausch von Informationen sowie Cyberkrisen- und Notfallübungen (Kapitel VI, Artikel 45)

BaFin hat Umsetzungshinweise zu IKT-Risikomanagement und Drittparteienrisikomanagement veröffentlicht.

BaFin wird BAIT/VAIT etc. aufheben.

DORA - Konkretisierung der Anforderungen – RTS/ITS (First Batch)

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Bereits vorliegende Fassungen zu:

- IKT-Risikomanagementrahmen
  - RTS zum IKT-Risikomanagementrahmen (Art. 15)
  - RTS zum vereinfachten IKT-Risikomanagementrahmen (Art. 16 Abs. 3)

- Behandlung, Klassifizierung und Berichterstattung zu IKT-bezogenen Vorfällen:
  - RTS zu Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen (Art. 18 Abs. 3)

- IKT-Drittparteienrisikomanagement
  - RTS zur Leitlinie in Bezug auf die Nutzung von IKT-Dienstleistungen (Art. 28 Abs. 10)

- EU-Überwachungsrahmenwerk

  - Delegierte Verordnung zu den Kriterien zur Festlegung der Kriterien für die Einstufung von IKT-Drittdienstleistern als kritisch für Finanzunternehmen (Art. 31 Abs. 6)
  - Delegierte Verordnung zur Festlegung der Höhe der von der federführenden Überwachungsbehörde bei kritischen IKT-Drittdienstleistern zu erhebenden Überwachungsgebühren und der Art und Weise der Entrichtung dieser Gebühren (Art. 43 Abs. 2)

DORA – Befugnisse der Aufsichtsbehörde

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Handlungsmöglichkeiten der nationalen Behörden (Deutschland: BaFin)

- **<u>Mindestens</u> folgende Befugnisse (Artikel 50 Abs. 2 DORA)**
  - 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;
  - Durchführung von Vor-Ort-Inspektionen oder Untersuchungen, einschließlich unter anderem der Vorladung von Vertretern der Finanzunternehmen, damit diese mündliche oder schriftliche Erklärungen zu Sachverhalten oder Unterlagen abgeben, die mit Gegenstand und Zweck der Untersuchung in Zusammenhang stehen, sowie der Aufzeichnung der Antworten
  - der Befragung jeder anderen natürlichen oder juristischen Person, die dieser Befragung zum Zweck der Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt;
  - das Verlangen von Korrektur- und Abhilfemaßnahmen bei Verstößen gegen die Anforderungen dieser Verordnung.

DORA – Sanktionsmöglichkeiten

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Welche Sanktionsmöglichkeiten müssen nationalen Aufsichtsbehörden übertragen werden?

- **<u>Mindestens</u> folgende Sanktionsmöglichkeiten (Artikel 50 Abs. 4)**:
  - die Erteilung einer Anweisung, wonach die natürliche oder juristische Person gegen diese Verordnung verstoßendes Verhalten zu unterlassen und von einer Wiederholung abzusehen hat;
  - das Verlangen, dass Praktiken oder Verhaltensweisen, die nach Ansicht der zuständigen Behörde den Bestimmungen dieser Verordnung zuwiderlaufen, vorübergehend oder dauerhaft eingestellt und nicht wiederholt werden;
  - das Ergreifen jeder Art von Maßnahme, auch finanzieller Art, um sicherzustellen, dass Finanzunternehmen weiterhin die rechtlichen Anforderungen erfüllen;
  - das Verlangen — soweit gemäß nationalem Recht zulässig — bereits existierender Aufzeichnungen von Datenübermittlungen im Besitz einer Telekommunikationsgesellschaft, wenn der begründete Verdacht auf einen Verstoß gegen die Verordnung besteht und diese Aufzeichnungen für eine Untersuchung von Verstößen gegen diese Verordnung relevant sein könnten;
  - die Abgabe öffentlicher Bekanntmachungen, einschließlich öffentlicher Bekanntgaben, in denen die Identität der natürlichen oder juristischen Person und die Art des Verstoßes angegeben sind.
- **<u>Maßnahmen nach Abs. 4 sollen auch gegen Mitglieder des Leitungsorgans verhängt werden können (Art. 50 Art. 5)</u>**

DORA – Stand zu den Sanktionen nach nationalem Recht

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Regelungen durch das Finanzmarktdigitalisierungsgesetz (FinmadiG) – Beispiel KWG, § 47a NEU

„§ 47a

Besondere Befugnisse nach der Verordnung (EU) 2022/2554

(1) Die Bundesanstalt kann bei Verstößen gegen die Verordnung (EU) 2022/2554 unbeschadet sonstiger in diesem Gesetz geregelter Befugnisse im Einzelfall Anordnungen treffen, die geeignet und erforderlich sind, um die Einhaltung der Vorgaben der Verordnung (EU) 2022/2554 im Anwendungsbereich dieses Gesetzes sicherzustellen. Sie kann gegenüber einem Institut insbesondere anordnen,

1. das gegen diese Verordnung verstoßende Verhalten zu unterlassen und von einer Wiederholung abzusehen,

2. Praktiken oder Verhaltensweisen, die den Bestimmungen der Verordnung zuwiderlaufen, vorübergehend oder dauerhaft einzustellen und nicht zu wiederholen,

3. sicherzustellen, dass weiterhin die rechtlichen Vorgaben erfüllt werden, und

4. Korrektur- und Abhilfemaßnahmen vorzunehmen.

(2) Die Bundesanstalt und die Deutsche Bundesbank können Untersuchungen über die Einhaltung der Vorgaben der Verordnung (EU) 2022/2554 im Anwendungsbereich dieses Gesetzes vornehmen. Unbeschadet sonstiger in diesem Gesetz geregelter Befugnisse kann die Bundesanstalt zu diesem Zweck Mitglieder der Organe eines Instituts zu einer Befragung vorladen, damit diese mündliche oder schriftliche Erklärungen zu Sachverhalten oder Unterlagen abgeben, die mit Gegenstand und Zweck der Untersuchung in Zusammenhang stehen, und die mündlichen Erklärungen aufzeichnen. § 44 Absatz 6 gilt entsprechend. Die Bundesanstalt kann die Durchführung der Befragung auf die Deutsche Bundesbank übertragen.“

DORA – Verstöße und Bußgelder

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Geplante Regelungen durch das Finanzmarktdigitalisierungsgesetz (FinmadiG) – Beispiel KWG, § 56 Abs. 5e NEU

„Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

einer vollziehbaren Anordnung nach

- Artikel 6 Absatz 5 Satz 3, Artikel 28 Absatz 3 Unterabsatz 4 oder Artikel 42 Absatz 6 Satz 1 oder
- Artikel 16 Absatz 2 Satz 3 oder Artikel 26 Absatz 1 Satz 2 zuwiderhandelt oder

- entgegen Artikel 19 Absatz 4 eine dort genannte Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,
- entgegen Artikel 26 Absatz 1 Satz 1 einen Test nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig durchführt
- entgegen Artikel 28 Absatz 3 Unterabsatz 3 einen Bericht nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet,
- entgegen Artikel 28 Absatz 3 Unterabsatz 5 die Behörde
  - über eine geplante vertragliche Vereinbarung bis zum Abschluss einer solchen Vereinbarung
  - unverzüglich über den Fall, dass eine Funktion kritisch oder wichtig geworden ist, nicht, nicht richtig oder nicht vollständig unterrichtet oder
- entgegen Artikel 45 Absatz 3 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.“

Bußgeldrahmen: bis zu 5 Mio. EUR

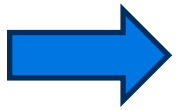
DORA – Drittparteienrisiko
Exkurs: Mindestvertragsinhalte

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

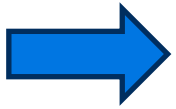
Verträge zwischen Finanzunternehmen und IKT-Drittdienstleister

Grundlagen:

- Art. 30 DORA
- RTS zur Leitlinie in Bezug auf die Nutzung von IKT-Dienstleistungen (Art. 28 Abs. 10)
- Final Report on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting **critical or important functions** (Article 30(5))



Die BaFin hat auf ihrer Website eine Übersicht darüber erstellt, welche Vertragsinhalte gem. Artikel 30 Abs. 2 einschließlich der RTS in den Vertrag mit aufgenommen werden müssen. Erbringt der IKT-Drittdienstleister kritische oder wichtige Funktionen, erweitern sich die Vertragsinhalte um die in Art. 30 Abs. 3 genannten Punkte



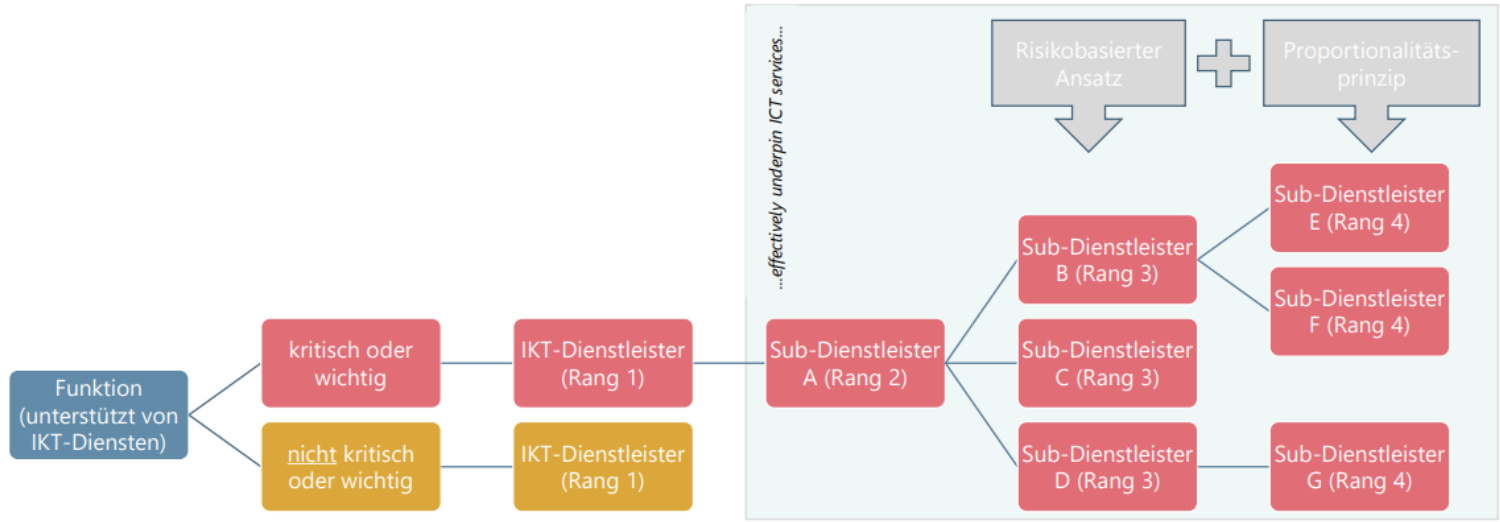
Finanzunternehmen sollten „DORA-Addendum“ mit ihren IKT-Drittdienstleistern abschließen

DORA – Drittparteienrisiko
Exkurs: Informationsregister

TeleTrusT Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Informationsregister zur Steuerung des Drittparteienrisikos

IKT-Dienstleister und ihre Unterauftragnehmer



Art. 3 Nr. 1 ITS: *Financial entities that maintain and update the register of information shall ensure that*

a. *the register of information includes the required information in relation to all the ICT services provided by direct ICT third-party providers; and*
b. *the register of information includes information on all subcontractors that effectively underpin ICT services supporting critical or important functions or material part thereof.*

BaFin

DORA Informationsregister

Quelle: BaFin

DORA – Aktuelle Fragen aus der Praxis

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Aktuelle Themenbereiche

- **Müssen Finanzunternehmen neben dem DORA auch NIS-2 beachten?**

  § 28 Abs. 5 Nr. 1 BSIG-E nimmt Finanzunternehmen von wesentlichen Pflichten aus, aber z.B. Registrierungspflicht bleibt in jedem Fall bestehen (§ 33 BSIG-E).

- **Inwieweit finden die Anforderungen aus dem DORA unmittelbar Anwendung auch auf IKT-Drittdienstleister?**

  DORA eröffnet in Art. 2 Abs. 1 lit. u) zwar den unmittelbaren Anwendungsbereich auch für IKT-Drittdienstleister, die Anforderungen in DORA richten sich jedoch überwiegend an das Finanzunternehmen

- **Müssen IKT-Drittdienstleister iSd Art. 2 Abs. 1 lit. u) DORA daneben auch NIS-2 beachten?**

  Beispiel: Saas-Anbieter können sowohl in den Anwendungsbereich von DORA („IKT-Drittdienstleister““) als auch in den Sektor „Digitale Infrastruktur“ (Anlage 1, Ziffer 6.1.4 zum BSIG-E) des BSIG-E fallen.

  Für Finanzunternehmen erklärt § 28 Abs. 5 Nr.1 BSIG-E wesentliche Normen aus dem BSIG für nicht anwendbar. Eine entsprechende Aussage in Bezug auf IKT-Drittdienstleister fehlt derzeit vollständig.

Q&A