TaylorWessing

DORA, NIS2, CRA – rechtliche Auswirkungen auf Unternehmen(sleitung)

15. Hamburger Financial Lines Forum am 17. Oktober 2025

Rechtsanwältin Dr. Gunbritt Kammerer-Galahn

DORA, NIS2, CRA – rechtliche Auswirkungen auf Unternehmen(sleitung)

Überblick

1 | Europas digitale Dekade

TaylorWessing

1 > Europas digitale Dekade

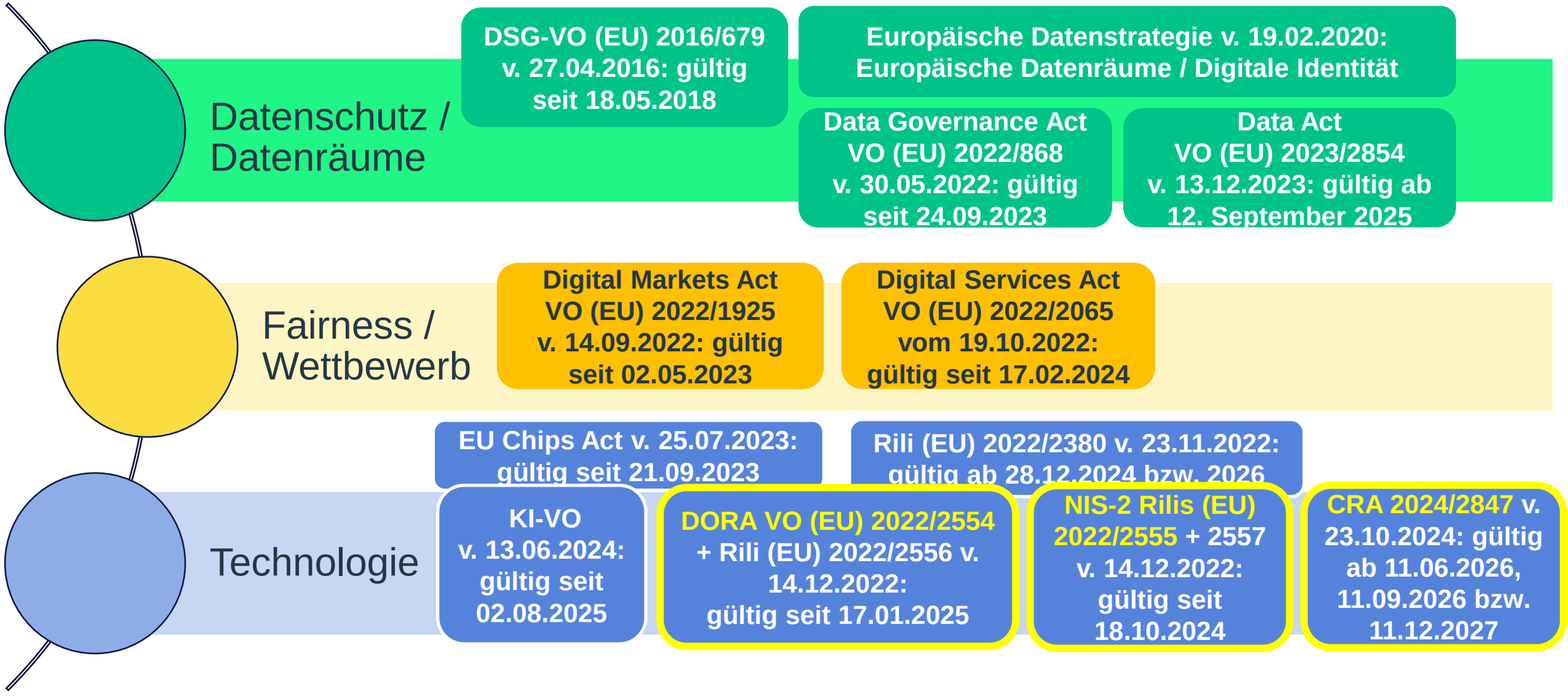
„Europas digitale Dekade bis 2030“

EU-Kommission entwickelt am 9. März 2021 während Corona-Pandemie „*Eine europäische Datenstrategie*“ vom 19. Februar 2020 weiter:

- **Eine offene, demokratische und nachhaltige Gesellschaft:** digitale Bildung und digitale Identität als Zugang für alle EU-Bürger:innen, Medien mit hochwertigen Inhalten / Medienpluralismus, Kreislaufwirtschaft für Geräte, Datenräume, Datenschutz
- **Eine faire und wettbewerbsfähige Wirtschaft:** Stärkung der globalen Wettbewerbsfähigkeit der EU-Wirtschaft, Schaffung eines Daten-Binnenmarkts, Überprüfung der Eignung der EU-Wettbewerbsregeln für das digitale Zeitalter
- **Technologie im Dienst der Menschen:** 5G- und 6G-Netze, Super- und Quantencomputer, Quantenkommunikation und Blockchain, Entwicklung und Einsatz von künstlicher Intelligenz, EU-Rechenzentren/-Cloudkapazitäten, EU-eigene Chip-Produktion, Normungsvereinheitlichung (z.B. ein Ladekabel mit USB-C-Anschluss für alle Geräte), ***Cybersicherheit und insbesondere die digitale und operationale Resilienz der Akteure in der EU***

1 > Europas digitale Dekade

Digitale Dekade der EU seit 2020:



2 | DORA

TaylorWessing

2 > DORA – Anwendungsbereich

Zeitlicher und persönlicher Anwendungsbereich

- **Inkrafttreten** am 16. Januar 2023 (Art. 64 DORA) und **Anwendung** in allen 27 EU-Mitgliedstaaten **seit 17. Januar 2025**
- **Anwendung auf Finanzunternehmen** (Art. 2 Abs. 1 DORA), insbesondere:
  - **Kreditinstitute** (lit. a)
  - **Versicherungs- und Rückversicherungsunternehmen** (lit. n), außer solche nach Art. 4 SII-Richtlinie:
    - Beitragseinnahmen (Rück-)VU p.a. ≤ EUR 5 Mio.
    - versicherungstechnische Rückstellungen (VU/Gruppe) ≤ EUR 25 Mio.
    - keine Haftpflicht-, Kredit-, Kautionsversicherungsrisiken und keine Rückversicherung mit Beitragseinnahmen p.a. > EUR 0,5 Mio.
  - **große (Rück-)Versicherungsvermittler (in Nebentätigkeit)**, außer:
    - Kleinst-, Klein- oder mittlere Unternehmen, also weniger als 250 MA und EUR 43 Mio. Jahresumsatz

2 > DORA – IKT-Risikomanagement

IKT-Risiken fortlaufend managen:

IKT-Risikomanagement (Kap. II Art. 5 - 16 DORA)

- **Verantwortung des Leitungsorgans**
- Solider, umfassender, gut dokumentierter **IKT-Risikomanagementrahmen** (Teil des Gesamtrisikomanagementsystems des VU)
- **Regelmäßige interne Revision** mit Follow-up-Verfahren
- **mind. 1x jährlich Dokumentation und Überprüfung**

Testen der digitalen operationalen Resilienz (Kap. IV Art. 24 - 27 DORA)

- solides umfassendes **Programm für das Testen**
- Tests durch **unabhängige Parteien** (intern oder extern)
- angemessene Tests **mind. 1x jährlich**: z.B. Schwachstellen-, Open-Source-,Lücken-, Netzwerksicherheits-Analysen, Quellcodeprüfungen
- Besonderer **Penetrationstest (TLPT) mind. alle 3 Jahre** durch sachkundigen Tester

Informationsaustausch zu Schwachstellen / Cyberrisiken (Kap. VI Art. 45 DORA)

- freiwilliger Austausch von Infos / Erkenntnissen **über Cyberbedrohungen**
- **Austauschvereinbarung** = rechtliche Basis, welche an BaFin zu melden ist
- denkbar: Austausch über **GDV** oder staatliche Behörden, also auch über die **BaFin** (= freiwillige Meldung nach Art. 19 DORA)

2 > DORA – IKT-Berichtspflichten und BaFin-Aufsicht

IKT-Berichtspflichten und -Aufsicht:

Berichterstattung über Vorfälle
(Kap. III Art. 17 - 23 DORA)

- **Prozess** für Behandlung IKT-bezogener Vorfälle und Cyber-bedrohungen
- **Frühwarnindikatoren**
- **Klassifizierung** nach Anzahl, Dauer, geografischer Ausbreitung, Datenverlusten, Kritikalität der betroffenen Dienste, den wirtschaftlichen Auswirkungen
- **Dokumentation / Meldung** *schwerwiegender* IKT-bezogener Vorfälle an BaFin-Portal (MVP)

Management von IKT-Drittdienstleisterrisiken
(Kap. V Art. 28 - 30 DORA)

- **Strategie für das IKT-Drittparteienrisiko**
- **stets aktuelles Informations-register mit allen Verträgen**, 1x jährlich Infos an BaFin
- geplante Verträge mit IKT-Drittdienstleister über **kritische oder wichtige Funktion/en vorab an BaFin** (Aufsicht entscheidet über Kritikalität!)
- **Vertrag** mit Drittdienstleistern hat **Mindestinhalte** zu regeln

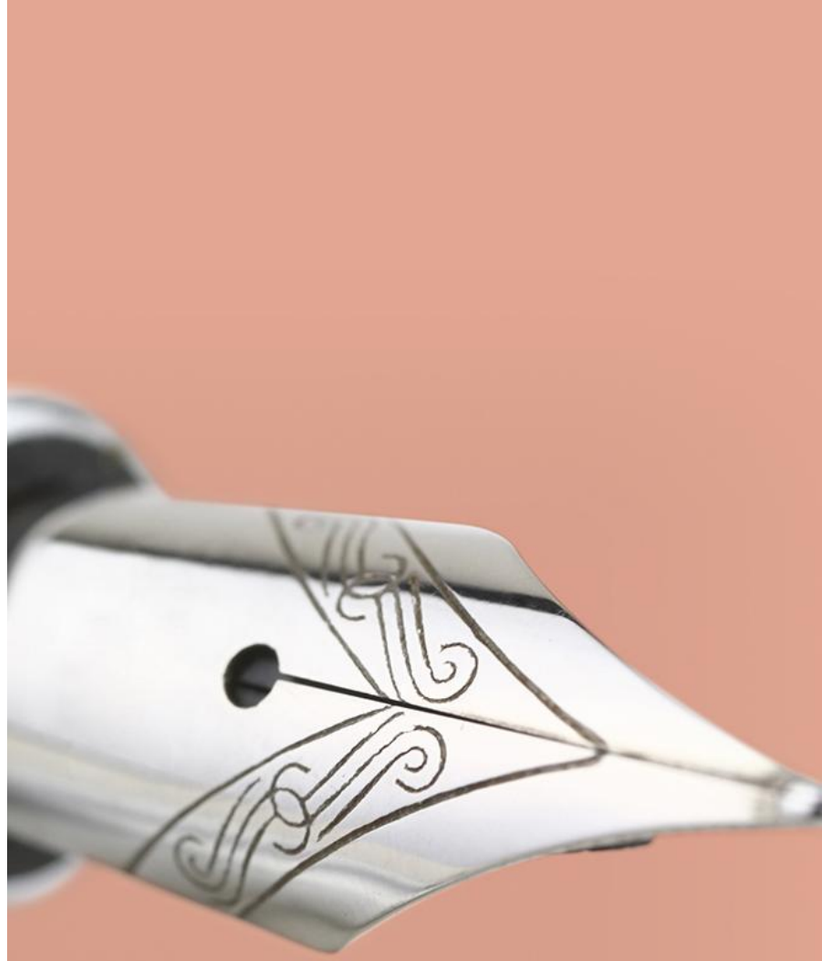
Überwachung kritischer IKT-Drittdienstleister
(Kap. V Art. 31 - 44 DORA)

- BaFin benennt 1x jährlich **kritische IKT-Drittdienstleister** je nach
  - systemischen Auswirkungen / Charakter, Abhängigkeit der VU, Grad der (fehlenden) Substituierbarkeit
  - nicht: gruppeninterne IKT-Dienstleister
- BaFin unterrichtet betr. IKT-Drittdienstleister; damit beginnt laufende entgeltliche Überwachung
- IKT-Dienstleister-Gruppe benennt jur. Person

2 > DORA – Anpassung Governance

Neuer IKT-Risikomanagementrahmen

- VAIT-Anforderungen sind **im Wesentlichen auch in DORA abgebildet**
- **Wesentliche Unterschiede** bei Governance und Organisation:
  - Zusatzanforderungen an das **Testen**
  - IKT-Risikomanagementrahmen weiter als IT-Strategie nach VAIT:
    - Neu: **unabhängige IKT-Risikokontrollfunktion**, der im VAIT vorgesehenen *Informationssicherheitsbeauftragten* entfällt
    - Neu: **Überwachungsfunktion zu IKT-Dienstleistungsverträgen** (neu einzurichten oder **Vorstand**, Art. 5 Abs. 3)
    - Neu: **Fortbildungspflicht von Vorstand + MA** zu DORA (Art. 5 Abs. 4)
  - **Alleinverantwortung** für wirksames und umsichtiges Management der IKT-Risiken liegt ausdrücklich beim **Vorstand** (Art. 5)



3 | NIS2-Richtlinien

3 > NIS2 – Überblick

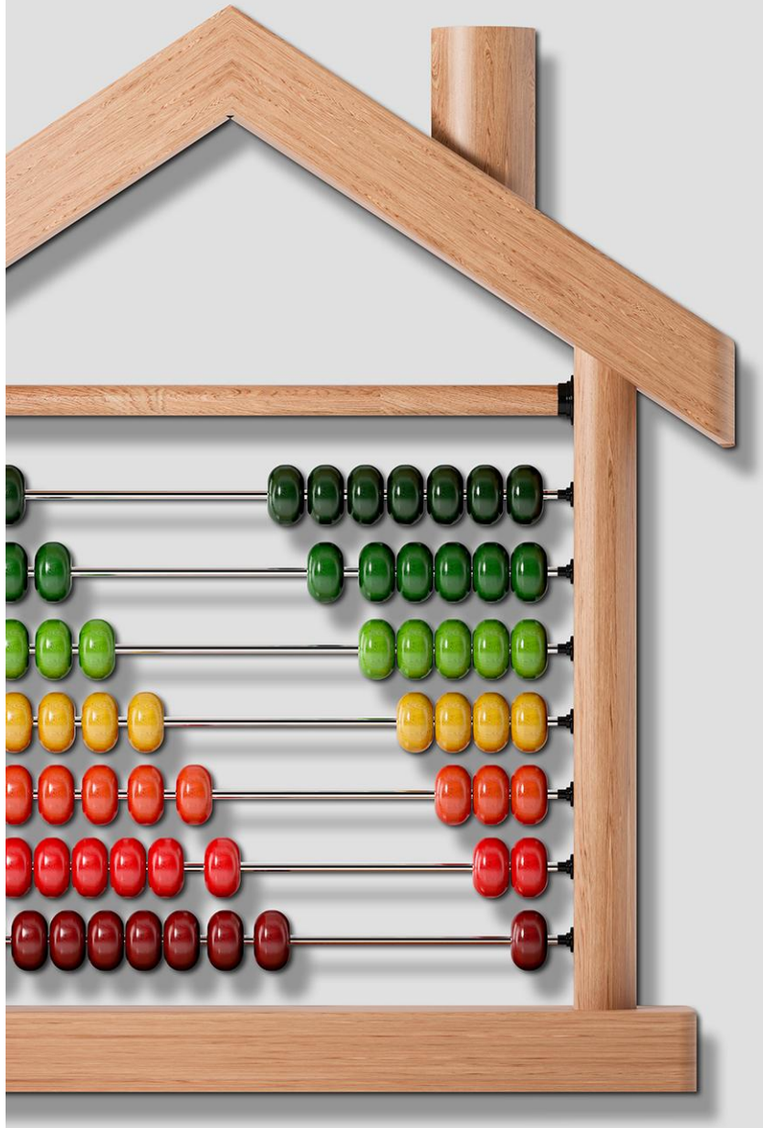
Richtlinie (EU) 2022/2555 (NIS2-Richtlinie)

- Überarbeitung der ursprünglichen Richtlinie (EU) 2016/1148 zur **Netzwerk- und Informationssicherheit** (NIS-Richtlinie)
- **Ziel:** Sicherstellung eines **hohen Cybersicherheitsniveaus** in der EU
- Inkrafttreten: 16. Januar 2023; **Umsetzung bis 18. Oktober 2024**, aber**:** noch keine dt. Umsetzung (insb. im BSIG und BSI-VOen)
- bestehende Standards wie der **IT-Grundschutz**, die **ISO/IEC 27001** und der Kriterienkatalog **Cloud Computing C5** werden möglicherweise nur einen Teil der neuen Anforderungen der NIS2-Richtlinie abdecken
- zusätzliche **technische und organisatorische Maßnahmen (TOMs)** werden erforderlich sein

3 > NIS2 – Anwendungsbereich

Richtlinie (EU) 2022/2555 (NIS2-Richtlinie)

- **Anwendung grundsätzlich auf**:
  - mittlere Unternehmen (50 – 249 MA) und
  - große Unternehmen (ab 250 MA)
- **Unabhängig von Größe: kritische Einrichtungen** (Art. 2 + Anhang I), insb.:
  - Energieversorgung, Luft-/Bahn-/Straßenverkehr/Schifffahrt, Banken und Börsen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastrukturen (Clouds, Internetknoten etc.), öfftl. Verwaltung, Strukturen für Weltraumfahrt
- **Unabhängig von Größe: sonstige kritische Sektoren** (Art. 2 + Anhang II), insb.:
  - Post- und Kurierdienste, Abfallbewirtschaftung, Chemieproduktion, Lebensmittelproduktion, verarbeitendes Gewerbe, Online-Marktplätze/-Suchmaschinen, Forschungseinrichtungen
- **Richtlinie (EU) 2022/2557 für kritische Einrichtungen** (physische Sicherheit)



3 > NIS2 – Verantwortlichkeiten

Verpflichtungen und Verantwortung der Geschäftsleitung

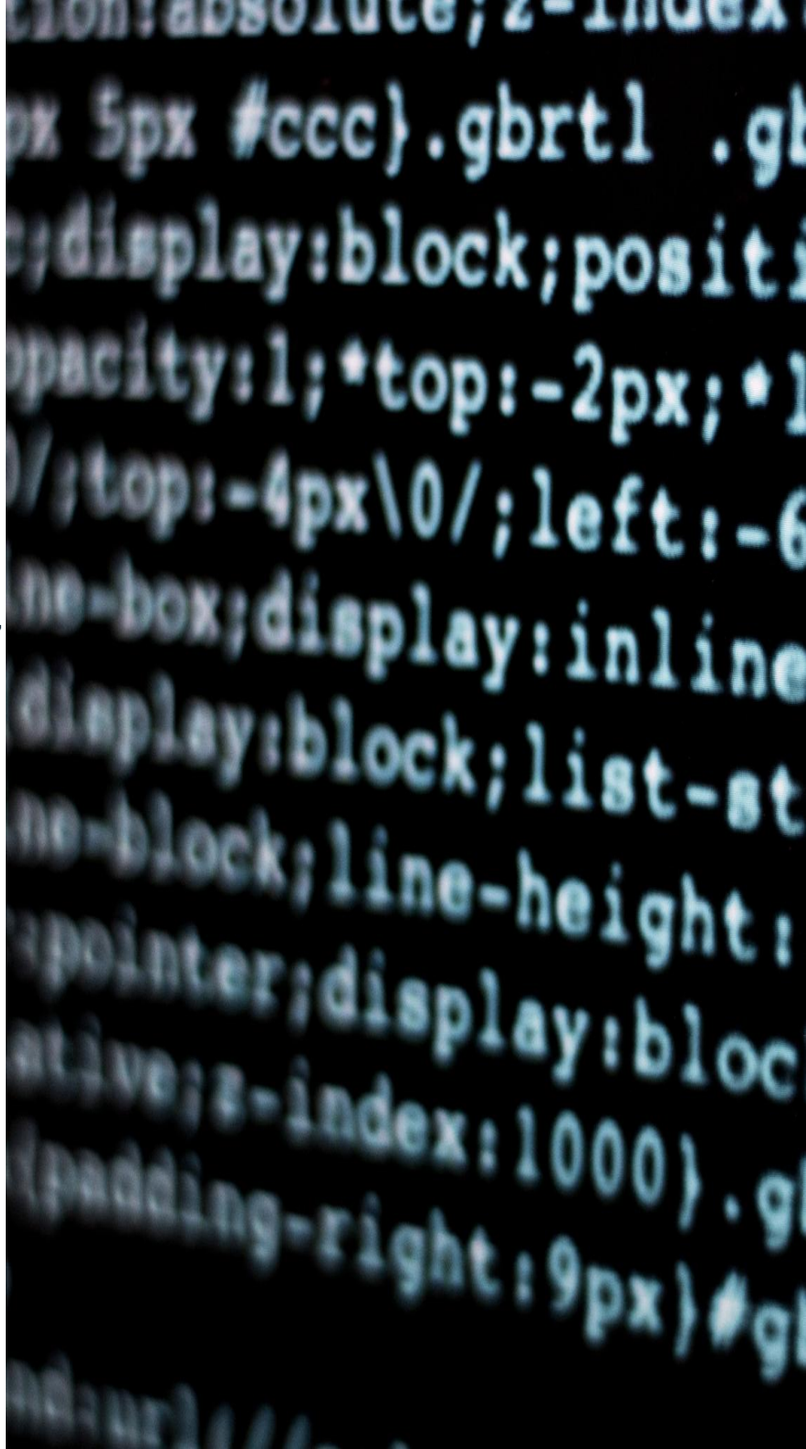
- **Risikomanagementmaßnahmen** (dazu können auch Testungen zählen) sind von den Leitungsorganen zu genehmigen und zu überwachen (Art. 20, 21); regelmäßige Schulungen der Leitungsorgane (Art. 20 Abs. 2)
- anders als DORA: kein entsprechendes IKT-Drittdienstleistermanagement
- **Berichtspflichten bzgl. erheblicher Sicherheitsvorfälle** (Art. 23)
- **Registrierung bei ENISA** und Zugriff durch nationale Stellen (Art. 27)
- **freiwilliger Informationsaustausch** zwischen den Einrichtungen und Einrichtung einer **EU-Schwachstellendatenbank** (Art. 12)
- **Geldbußen** mind. EUR 7 Mio. (wesentliche Einrichtung) bzw. EUR 10 Mio. (wichtige Einrichtung) oder 1,4% bzw. 2% des weltweiten Jahresumsatzes (Art. 34)
- **Leitungsorgane** tragen die **Gesamtverantwortung** (Art. 20 Abs. 1)

4 | Cyber-Resilienz-Verordnung (CRA)

4 > CRA – Überblick

Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen

- **Ziel:** Rechtlichen Rahmenbedingungen für die Entwicklung sicherer Produkte in der EU hinsichtlich deren Cyber-Resilienz
- **Inkrafttreten**: 10. Dezember 2024; **Anwendbarkeit** grds. ab 11. Dezember 2027 aber Einrichtung der nationalen Meldestellen bis 11. Juni 2026 und Meldepflichten der Hersteller ab 11. September 2026
- **Wesentliche Pflicht**: Hersteller meldet jede aktiv ausgenutzte Schwachstelle, die im Produkt mit digitalen Elementen enthalten ist und von der er Kenntnis erlangt, an Meldeplattform zusammen mit Korrektur- oder Risikominderungsmaßnahmen, die Nutzer ergreifen können (Art. 14)
- **keine spezifischen Regelungen zur Geschäftsleiterhaftung**



5 | Zusammenfassung

TaylorWessing

5 > Take-aways

- **DORA, die NIS2-Richtlinien und auch der CRA** bringen bezüglich der Cybersicherheit zahlreiche neue Anforderungen insbesondere an die Geschäftsorganisation in VU und Einrichtungen anderer Industriesektoren:
  - umfangreiches Risikomanagement
  - regelmäßige Schulungen und Überprüfungen
  - strikte Meldepflichten
- Pflichtverletzung wird mit **hohen Geldbußen** sanktioniert
- DORA und NIS2-Richtlinie regeln ausdrücklich die Haftung der Geschäftsleitung
- CRA regelt nicht ausdrücklich eine Geschäftsleitungshaftung, aber Haftung folgt aus Verletzung der erweiterten Sorgfaltspflichten, § 43 Abs. 2 GmbHG, § 93 Abs. 2 AktG

► **D&O-Versicherer** und **Cyber-Versicherer** haben diese neuen Risiken beim Underwriting jeweils zu berücksichtigen

Europe > Middle East > Asia

taylorwessing.com