HSW | RECHTSANWÄLTE
HARDER SEDLMEIER WEITZEL

Mandanteninformation

Sachgerechte Vorbereitung auf DORA

Vor mehr als einem Jahr trat am 16. Januar 2023 – weitgehend unbemerkt – eine für Betroffene enorm folgenreiche EU-Vorschrift in Kraft. Da die Umsetzung so aufwendig ist, hat der Gesetzgeber eine zweijährige Umsetzungsfrist vorgesehen. Wer klug war, hat die Vorbereitung auf die Umsetzung von DORA sofort gestartet. Denn zum 16.1.2025 treten alle Pflichten aus der Vorschrift in Kraft – ohne jegliche Übergangsfrist!

Einige Unternehmen und Mandanten beginnen erst jetzt mit ihren Vorbereitungen. Und was passiert dabei: Angesichts von Umfang und Kosten der Vorbereitung sinkt bei vielen Mut oder Engagement. Das ist jedoch fatal!

Lesen sie hier, wie und weshalb Sie die Vorbereitung angehen und *sofort* starten sollten.

Hintergrund

Digitalisierung ist ein Modewort. Lange als Heilsbringer oder Universalmittel zur Steigerung von Effizienz und Gewinn angepriesen, macht sich inzwischen Ernüchterung breit: Ausfallrisiken durch Hacker und sogenannte „Cyber-Angriffe“ oder „Cyber-Risiken“ zwingen zu immer aufwendigeren Schutzmaßnahmen.

Da kommt ein weiteres Modewort recht: Resilienz beschreibt die Eigenschaft mancher Stoffe, nach extremer Verformung wieder in den Urzustand zurückzukehren. Gummi ist ein solches Material. Resilienz umschreibt heute die Fähigkeit, sich durch Widrigkeiten und Angriffe nicht aus der Bahn werfen zu lassen.

Genau das verspricht sich die EU von dem am 16.1.2023 in Kraft getretenen Digital Operational Resilience Act (kurz „DORA“, amtlich Verordnung (EU) 2022/2554 vom 14.12.2022 über die digitale operationale Resilienz im Finanzsektor). Cyber-Resilienz soll dafür sorgen, dass für die Funktion der Finanzmärkte wichtige Unternehmen durch Ausfälle oder Manipulation ihrer IT unbeeinflusst bleiben und nahtlos weiter operieren können – so weit der Traum.

Schafft DORA Vereinfachung oder Vereinheitlichung?

Leider nein! Finanz- und Versicherungsunternehmen unterliegen je nach Branche verschiedenen aufsichtsrechtlichen Regeln Allein zur IT hat die BaFin mit ihren Rundschreiben BAIT, KAIT, ZAIT und VAIT bzw. der MaRisk (BA) für jede Branche teils ähnliche, teils unterschiedliche Regeln aufgestellt. Im Geschäft oft zwingende Normen wie ISO/IEC 20000 oder 27001 und nationale Gesetze wie BSIG und die zugehörige BSI-Kritisverordnung treten hinzu.

Mit Recht beklagt die Industrie deshalb eine komplexe Regulatorik mit enormen Kosten und Herausforderungen bei der Umsetzung.

DORA besorgt nur die Vereinheitlichung nationaler Vorschriften für sichere IT-Systeme im Finanzsektor. Auch wenn die Vorschrift neben viele weitere tritt, ein Positives hat sie: Anders als viele neue Gesetze ist DORA sehr konkret und gut verständlich geschrieben.

Praxistipp:	*Lassen Sie sich von den vielen Ratgebern und Websites nicht verwirren: In der Verordnung sind alle Pflichten klar und verständlich aufgezählt. Und die sind viel umfangreicher, als manche Ratgeber suggerieren!* *Lesen Sie die Verordnung daher unbedingt einmal vollständig durch. Ohne deren Kenntnis geraten Sie schon beim Start in Schieflage.*

Compliance-Risiko DORA

Wenn plötzlich so viele neue Pflichten, Kontrollen und Berichte eingeführt werden müssen – alles unter erheblicher Bußgeldandrohung – haben betroffene Unternehmen enormen Handlungsdruck.

Der wird durch DORA noch verschärft: Dem EU-Gesetzgeber war bewusst, welchen Aufwand die Umsetzung der neuen Pflichten schafft. Er schreibt deshalb ausdrücklich Projekte mit verbindlichen Zeitplänen und Steuerung durch Vorstand bzw. Geschäftsführung vor.

Praxistipp:	*Nehmen Sie die gesetzlichen Vorgaben zur Projektgestaltung ernst! Dieses Projekt kann nicht einfach an Externe, Einkauf oder IT-Abteilung weg-delegiert werden. An vielen Stellen ist die Beteiligung von Vorstand/GF und anderen Funktionen im Unternehmen zwingend vorgeschrieben.*

Wie lange dauert die Vorbereitung auf DORA?

Große Banken oder Versicherungen haben deshalb schon seit einem Jahr mit der Vorbereitung begonnen. In einem globalen Versicherungskonzern ist das zugehörige Projekt bis 2025/2026 geplant – rascher lassen sich die vielen neuen Anforderungen nicht weltweit umsetzen.

Je nach Größe des Unternehmens ist mit 1 bis 2,5 Jahren Vorbereitungszeit zu rechnen. Naturgemäß hängt die Zeitdauer stark mit dem Personaleinsatz im Vorbereitungsprojekt zusammen. Oft treten deshalb externe Berater auf den Plan, die Personalengpässe und fehlendes Know-How im Unternehmen ausgleichen.

Praxistipp:	*Sollten Sie von DORA betroffen sein und noch kein Vorbereitungs-Projekt aufgesetzt haben, fangen Sie sofort mit der Planung an!*

Was kostet die Vorbereitung auf DORA?

Das lässt sich für keinen der Betroffenen pauschal sagen. Es hängt auch davon ab, wie weit IT-Sicherheit, Cyber-Resilienz und Dokumentation im Unternehmen bereits entwickelt sind.

Ein gewollter Nebeneffekt von DORA: Nun kommt es zum Schwur, ob ein Unternehmen seine IT-Systeme und -Prozesse genügend ausfallsicher angelegt hat.

> ***Praxistipp:*** *Als erster Schritt zur Vorbereitung müssen Sie Ihre Lücken (neudeutsch „Gaps“) ermitteln. Daraus ergibt sich der Handlungsbedarf und die daraus folgende Budget-Planung!*

Die praktische HSW-Checkliste zeigt Ihnen auf, wie viele Vorgänge und Neuerungen im Unternehmen anstehen. Viele davon werden vorübergehend und einige dauerhaft zusätzliche Organisationen, Prozesse und Personal-Ressourcen benötigen.

> ***Praxistipp:*** *Unterschätzen Sie nicht den Budgetbedarf, planen sie ihn rechtzeitig und sorgen Sie für ausreichende und pünktliche Bereitstellung der Mittel! Ansonsten begehen Sie schon in der Vorbereitung den ersten Compliance-Verstoß.*

Was sind die größten Budget-Posten bei der Vorbereitung auf DORA?

- Notwendige Anpassungen an Segmentierung und Abschottung der Netzinfrastruktur (Hardware, Software und externe Dienstleister)
- Erstellung des Informationsregisters über alle vertraglichen Vereinbarungen mit IKT-Drittdienstleistern mit angemessener Dokumentation; im Zuge dessen Ermittlung der IKT-Verträge mit Anpassungsbedarf
- Mehrkosten durch zwingende Neu- oder Nachverhandlung der Verträge mit IT-Dienstleistern, um die vorgeschriebenen Inhalte einzufügen
- Ausreichend Ressourcen und Kapazitäten zur Überwachung von Nutzeraktivitäten und das Auftreten von IKT-Anomalien und IKT-Vorfällen
- Herstellung der Redundanz aller IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen zur Deckung des Geschäftsbedarfs
- Solides und umfassendes Programm für das Testen der digitalen operationellen Resilienz (erfordert bei großen Unternehmen zweistellige Millionenbeträge pro Jahr)
- Ausreichend komplexe, obligatorische Programme der Mitarbeiterschulung zur Sensibilisierung für IKT-Sicherheit und digitalen operationellen Resilienz

Ist DORA eine Aufgabe für die IT-Abteilung?

Auf keinen Fall darf die Vorbereitung zur Umsetzung an IT oder Einkauf weg-delegiert werden. Schon im Vorbereitungsprojekt *müssen* Vorstand bzw. Geschäftsführung beteiligt werden, bei Aufsichtsgremien und Wirtschaftsprüfern ist das dringend zu empfehlen. DORA legt genau fest, welche Leitungsorgane und Fachbereiche einzubeziehen sind.

Praxistipp: *Setzen Sie unbedingt ein Gesamtprojekt auf Ebene der Konzernmutter vor. Beteiligen Sie Aufsichtsgremien und Wirtschaftsprüfer. IT, QM, Einkauf und Rechtsabteilung sind in Teilprojekten zwingend mit einzubeziehen. Weitere Bereiche wie HR (für Schulungen) sind je nach Bedarf einzubinden.*

Die Gesamtverantwortung muss beim Leitungsorgan verbleiben, an das der Projektleiter direkt berichten sollte.

Welche Dokumente sind für DORA zu erstellen?

Die folgende Liste zeigt, wie umfangreich die neu zu erstellende bzw. überarbeitende Dokumentation ist. Diese ist regelmäßig und nachweisbar zu überprüfen und anzupassen. Die meisten Konzepte müssen laufend Tests unterzogen werden, die Tests müssen geplant und budgetiert werden.

Folgende Konzepte und Methoden sind gesondert zu dokumentieren:

1. Umfassende IKT-Geschäftsfortführungsleitlinie als eigenständige spezielle Leitlinie
2. *Als Teil der IKT-Geschäftsfortführungsleitlinie:* Spezielle Pläne für Eindämmungsmaßnahmen, Prozesse und Technologien für IKT-bezogene Vorfälle und Vermeidung weiterer Schäden
3. *Als Teil der IKT-Geschäftsfortführungsleitlinie:* Maßgeschneiderte Verfahren zur Reaktion und Wiederherstellung gemäß Art. 12 DORA
4. *Als Teil der IKT-Geschäftsfortführungsleitlinie:* Kommunikations- und Krisenmanagementmaßnahmen zur effektiven Informationsübermittlung gemäß Art. 14 und Meldung an zuständige Behörden gemäß Art. 19 DORA
5. IKT-Reaktions- und Wiederherstellungspläne (oft vorhanden, aber anzupassen)
6. Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen (oft vorhanden, aber anzupassen)
7. Richtlinien und Verfahren für die Datensicherung (oft vorhanden, aber anzupassen)
8. Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung von Daten
9. Zeitvorgaben für Wiederherstellungszeit und Wiederherstellungspunkte jeder Funktion zur Sicherstellung der vereinbarten Dienstleistungsgüte in Extremszenarien
10. Entwicklung der IKT-Risiken im Zeitverlauf, insbesondere Häufigkeit, Art, Ausmaß und Entwicklung von IKT-Vorfällen um Risikoausmaß zu verstehen und Cyberreife und Abwehrbereitschaft des Unternehmens zu verbessern
11. Ausreichend komplexe, obligatorische Programme der Mitarbeiterschulung zur Sensibilisierung für IKT-Sicherheit und digitalen operationellen Resilienz
12. *Außer bei Kleinstunternehmen:* Ergebnisse der Überwachung einschlägiger technischer Entwicklungen und neuester Prozesse für IKT-Risikomanagement zur wirksamen Abwehr von Cyberangriffen
13. Prozess für die Erfassung von IKT-Vorfällen und erheblichen Cyberbedrohungen mit allen Anforderungen nach Art. 17 Abs. 3 DORA

14. Prozess für die Behandlung IKT-bezogener Vorfälle
15. Klassifizierung von IKT-Vorfällen und Bestimmung ihrer Auswirkungen nach Kriterien in Art. 18 Abs. 1 DORA
16. Einstufung von Cyberbedrohungen nach Kritikalität gemäß Art. 18 Abs. 2 DORA
17. Details zum Meldewesen für schwerwiegende IKT-Vorfälle an zuständige Behörde
18. Mechanismen zur Information über schwerwiegende IKT-Vorfälle mit Auswirkungen auf finanzielle Interessen von Kunden (inkl. deren Prüfung) und ergriffene Maßnahmen an Kunden
19. Mechanismen zur Information potenziell betroffener Kunden über angemessene Schutznahmen, die jene ergreifen können, wenn erhebliche Cyberbedrohungen vorliegen
20. Solides und umfassendes Programm für das Testen der digitalen operationellen Resilienz gemäß Art. 25 bis 27 DORA
21. *Außer Kleinstunternehmen:* Verfahren und Leitlinien zur Priorisierung, Klassifizierung und Behebung aller bei Tests der digitalen operationellen Resilienz gemäß Art. 25 bis 27 DORA auftretenden Probleme
22. *Außer Kleinstunternehmen:* Interne Validierungsmethoden um sicherzustellen, dass alle bei Tests der digitalen operationellen Resilienz gemäß Art. 25 bis 27 DORA ermittelten Schwächen, Mängel oder Lücken vollständig angegangen werden
23. Strategie für das IKT-Drittparteienrisiko mit einer Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die durch IKT-Drittdienstleister bereitgestellt werden
24. Auditplan inkl. Art und Frequenz von IKT-Dienstleister-Audits auf Grundlage eines risikobasierten Ansatzes
25. Liste der IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen
26. Ausstiegsstrategie für alle IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen
27. Umfassend dokumentierte Ausstiegspläne für alle IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen
28. Planung von Alternativlösungen und Übergangsplänen, um IKT-Dienstleistern Dienstleistungen und Daten zu entziehen und sicher und vollständig an andere Dienstleister oder in eigene Systeme zu überführen
29. Angemessene Notfallmaßnahmen zur Fortführung der Geschäftstätigkeit, wenn bei IKT-Drittdienstleistern Risiken oder Fehler auftreten

Praxistipp: *Stellen Sie möglichst in der ersten Phase Ihrer DORA-Vorbereitung sicher, dass alle vorstehenden gesetzlich geforderten Dokumente in Ihrem Unternehmen vorliegen! Einige werden in Grundzügen existieren, aber zahlreiche werden oder grundlegend neu zu erstellen sein.*

Was sind die größten Herausforderungen bei der Vorbereitung auf DORA?

Eine Auswertung laufender DORA-Vorbereitungs-Projekte zeigt immer wieder folgende Probleme:

- Änderungsaufwand in der Organisation wird unterschätzt:
  - Unternehmen versuchen, die neuen Pflichten in bestehende Organisationen und Prozesse einzufügen.
  - Es braucht aber zum Teil neue Gremien, Abläufe und Steuerungsfunktionen.
- Kosten-, Zeit- und Personalaufwand wurden massiv unterschätzt:
  - Die Mitarbeiter im Kernprojekt entfallen auf Monate bis Jahre für das Tagesgeschäft.
  - Neue Software, redundant auszulegende Systeme, externe Berater und teurere IT-Verträge benötigen erhebliche Zusatzbudgets. Wer parallel zur DORA-Vorbereitung im IT-Budget Einsparungen vorsieht, droht zu scheitern.
- Fehlendes „Commitment“:
  - Ermüdet von DSGVO-Vorbereitungsprojekten und anderen IT-Projekten, lässt das Engagement der meisten Vorstände und Organisationseinheiten nach anfänglicher Begeisterung rasch nach.
  - Die monatelange Planung und Vorbereitung des Projektes ist indes der geringste Aufwand. Die Durchführung des Projektes erfordert noch wesentlich mehr Engagement und Energie.
- Dokumentationsaufwand wird vernachlässigt:
  - Die Erstellung von Dokumenten wird gern in das Qualitätsmanagement verlagert. Allerdings ist jenes nur für vollständige Dokumentation bestehender Prozesse zuständig.
  - Für DORA müssen ganz neue Prozesse und Kontrollmechanismen erst entworfen, dann getestet und angepasst werden.
  - Der von DORA vorgeschriebene Dokumentationsaufwand ist immens und wird oft unterschätzt.

Wie kann ich die Vorbereitung auf DORA planen?

Dazu stellen wir auf unserer Homepage laufend aktualisierte Checklisten und Tools zum Download bereit.

Eine Prüfliste für die Vorbereitung in allen Unternehmensbereichen liegt bereits vor. Für den Bereich Einkauf ist diese bereits als Tool zur Messung des Fertigstellungsgrades ausgearbeitet. Das erleichtert Planung und Berichterstattung im Projektablauf.

Ihre Ansprechpartner für dieses Thema:

Rechtsanwalt Bernd H. Harder
Rechtsanwalt Dr. Christian Weitzel