ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

Update zum Digital Operational Resilience Act (DORA)

Karl Machan, CRM
Experte
Wertpapierunternehmen und Finanzinnovationen
Wien, 08. Mai 2025

FMA-DIALOG 2025
DORA - DIGITAL OPERATIONAL RESILIENCE ACT

- **Inkrafttreten**
  - DORA-Verordnung (EU) 2022/2554 ist 16. Jänner 2023 in Kraft getreten und ist seit 17. Jänner 2025 anzuwenden.
- **Wesentliche Regelungen**
  - Risikomanagement im Bereich Informations- und Kommunikationstechnologien (IKT)
  - Meldung von IKT-bezogenen Vorfällen an Behörden
  - Testen der digitalen operationalen Resilienz
  - Management des Risikos von IKT-Drittdienstleistern

Risikomanagement im Bereich Informations- und Kommunikationstechnologien (IKT)

Vereinfachter IKT-Risikomanagementrahmen (Artikel 16):

Wesentliche Inhalte:

- solider und dokumentierter IKT-Risikomanagementrahmen:
  - Risikoidentifikation, Risikoanalyse, Risikobewertung
  - Maßnahmen zur Minderung der Risiken
- Überwachung der Sicherheit und das Funktionieren der IKT-Systeme muss gewährleistet sein
- Einsatz von soliden, resilienten und aktualisierten IKT-Systemen, -Protokolle und –Tools zur Risikominimierung. Dabei sind vor Allem sind Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten zu berücksichtigen
- Ermittlung von wesentlichen Abhängigkeiten von IKT-Drittdienstleistern
- Erstellung von Geschäftsfortführungspläne sowie Gegen- und Wiederherstellungsmaßnahmen, um die Kontinuität der kritischen oder wichtigen Funktionen im Unternehmen zu gewährleisten und regelmäßig zu testen

Update zu IKT-bezogene Vorfälle

- Meldung seit 17.01.2025 verpflichtend:
  - FMA-Weit: 38 Meldungen
  - WPF: 1 Meldung

- Klassifizierung von IKT-bezogenen Vorfällen und erheblichen Cyberbedrohungen (Art. 18)
  - Kriterien zur Klassifizierung von Vorfällen in DelVO (EU) 2024/1772 geregelt
  - Delegierte Verordnung (EU) 2024/1772 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554

DORA - DIGITAL OPERATIONAL RESILIENCE ACT

Klassifizierungsansatz:

Verpflichtendes Kriterium
Kritikalität der betroffenen Dienste

& zusätzlich entweder

I. Erfolgreicher, böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme, sofern dieser zu Verlusten von Daten führen kann.

II Überschreitung d.er Schwellenwerte von mindestens zwei weiteren Kriterien:
Betroffene Kund:innen, finanzielle Gegenparteien oder Transaktionen
Reputationsschaden
Dauer und Ausfallzeiten des Vorfalls
Geografische Ausbreitung
Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten
Wirtschaftliche Auswirkungen

DORA - DIGITAL OPERATIONAL RESILIENCE ACT

Kriterium DelVO (EU) 2024/1772	Schwellenwerte
Kritikalität der betroffenen Dienste	**Jede Auswirkung** auf kritische Dienste a) zur Unterstützung kritischer oder wichtiger Funktionen b) die eine Konzession oder Registrierung erfordern bzw. beaufsichtigt werden c) sofern ein erfolgreicher, böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme vorliegt
Verluste von Daten	**a) Jede Auswirkung** auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten, sofern dies negative Auswirkungen auf die Umsetzung der Geschäftsziele oder Erfüllung der regulatorischen Anforderungen hat **b) Jeder erfolgreiche, böswillige und unbefugte Zugriff auf Netz- und Informationssysteme**, welcher **nicht unter Punkt a)** fällt und zu einem **Datenverlust führen kann**

DORA - DIGITAL OPERATIONAL RESILIENCE ACT

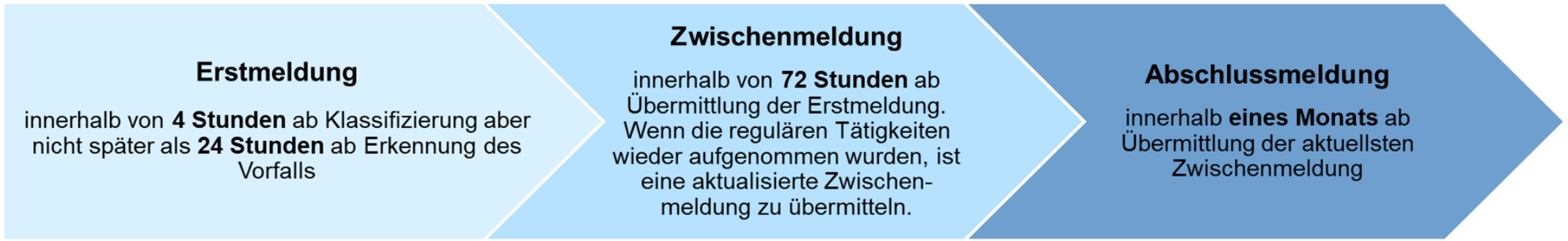
Kriterium DelVO (EU) 2024/1772	Schwellenwerte
Kunden, finanzielle Gegenparteien und Transaktionen	a) > 10 % aller Kunden, welche diesen Service nutzen b) > 100.000 Kunden c) > 30 % aller zentralen Gegenparteien d) > 10% der üblichen durchschnittlichen Anzahl an Transaktionen e) > 10% des üblichen durchschnittlichen Transaktionsvolumens f) alle festgestellten Auswirkungen auf Kunden oder finanzielle Gegenparteien, die vom Finanzinstitut als relevant eingestuft werden
Dauer und Ausfallzeiten	➢ > 24 Stunden ➢ > 2 Stunden bei kritischen Funktionen, sofern keine kürzere Dauer aufgrund anderer EU-Regularien vorgeschrieben ist
Wirtschaftliche Auswirkungen	➢ die direkten und indirekten Bruttokosten und -verluste überschreiten **EUR 100 000** oder werden voraussichtlich **EUR 100 000** überschreiten

DORA - DIGITAL OPERATIONAL RESILIENCE ACT

Kriterium DelVO (EU) 2024/1772	Schwellenwerte
Geografische Ausbreitung	➢ Liegt vor (Betroffenheit von mindestens zwei MS)
Reputationsschäden	Grad der Bekanntheit des Vorfalls beispielsweise: ➢ Medienaufmerksamkeit ➢ Nichterfüllung der aufsichtlichen Anforderungen ➢ Kundenverlust, mit Auswirkungen auf das Geschäft

FMA-DIALOG 2025
DORA - DIGITAL OPERATIONAL RESILIENCE ACT

- Fristen



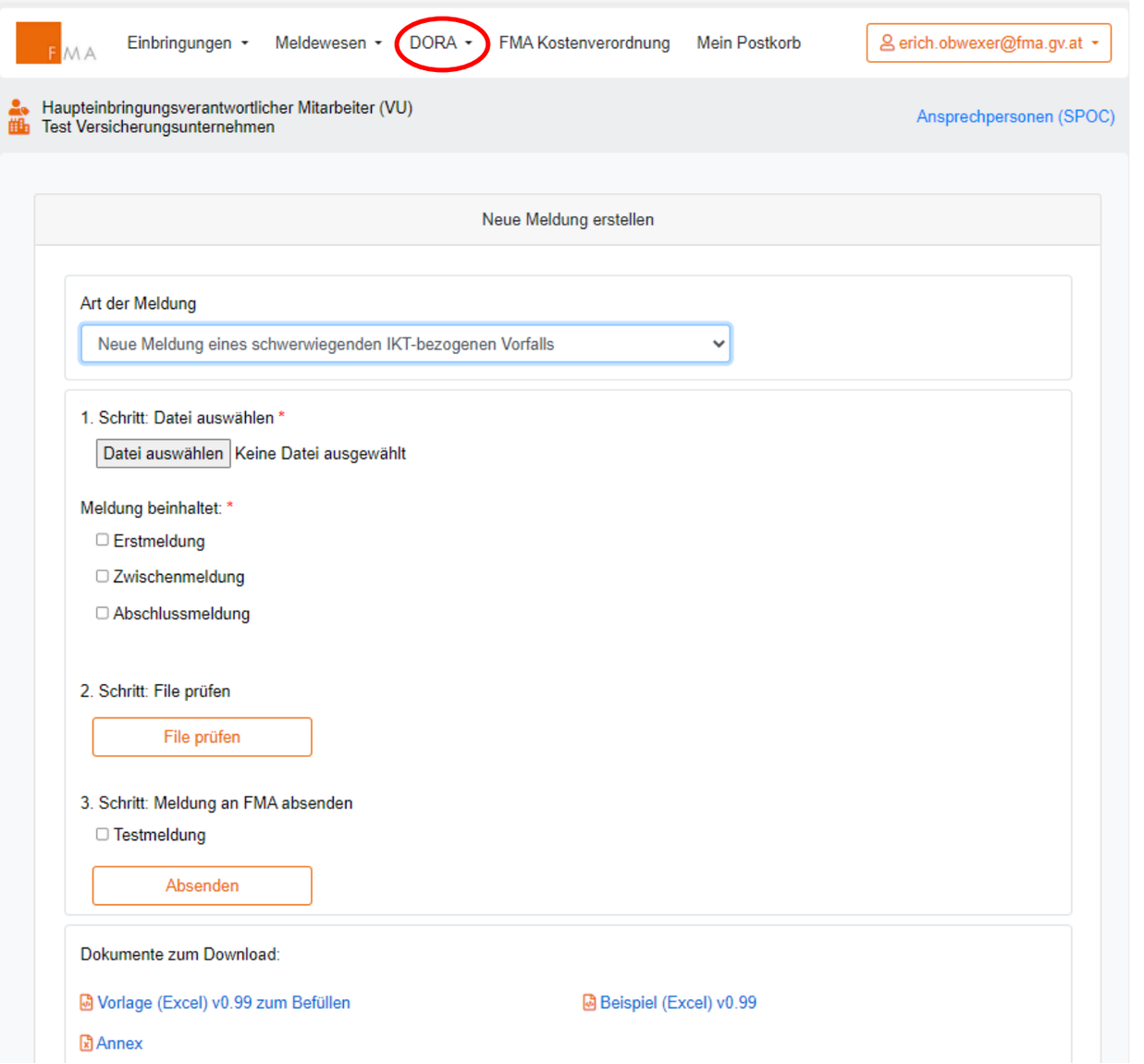
Wochenend- und Feiertagsbestimmungen: verlängerte Meldefristen bis 12 Uhr des nächsten Arbeitstages

- Freiwillige Meldung erheblicher Cyberbedrohungen

FMA-DIALOG 2025
DORA - DIGITAL OPERATIONAL RESILIENCE ACT

Meldungen: IKT-bezogene Vorfälle

- Meldeweg: FMA Incoming-Plattform
- Formular für die Einmeldung
- Weiterleitung an ESAs (EBA, EIOPA, ESMA), EZB, NIS-Behörde, …



Testen der digitalen operationalen Resilienz

Art 24 - allgemeine Anforderungen für Prüfungen der Betriebsstabilität digitaler Systeme

- Finanzunternehmen haben ein umfassendes Programm zur Prüfung der digitalen Betriebsstabilität im Rahmen des IKT-Risikomanagementrahmens zu erstellen und zu implementieren
- Prüfungen sind von unabhängigen internen oder externen Prüfern durchzuführen. Bei internen Prüfer: Sicherstellung ausreichender Ressourcen und Berücksichtigung allfälliger Interessenskonflikte
- Festlegung eines Follow-Up-Prozesses
- Prüfung bei IKT-Systemen, die kritische oder wichtige Funktionen unterstützen: mindestens einmal jährlich

Testen der digitalen operationalen Resilienz

Art 25 – Testen von IKT-Tools und -Systemen

- Das Programm umfasst je nach Kriterien des Unternehmens angemessene Tests wie etwa:
  - Schwachstellenbewertung und -scans
  - Open-Source-Analysen
  - Netzwerksicherheitsbewertungen
  - Lückenanalysen
  - Überprüfungen der physischen Sicherheit
  - Fragebögen und Scans von Softwarelösungen
  - Quellcodeprüfungen soweit durchführbar
  - Szenariobasierte Tests
  - Kompatibilitätstests
  - Leistungstests
  - End-to-End-Tests
  - Penetrationstests

Management des IKT-Drittparteienrisikos

- IKT-Drittparteienrisiko ein integraler Bestandteil des IKT-Risikos
- Finanzunternehmen bleiben jederzeit in vollem Umfang für die Einhaltung gesetzlichen Verpflichtungen verantwortlich
- Führen eines Informationsregisters (Unterscheidung kritischer und wichtige bzw. nicht kritischer und wichtige Funktionen)
- Jährliche Berichterstattung an FMA
- Ad-hoc-Meldung über jede geplante vertragliche Vereinbarung an FMA
- Vor Abschluss einer vertraglichen Vereinbarung Durchführung einer Due-Diligence-Überprüfung
  - handelt es sich um eine kritische oder wichtige Funktion
  - Beurteilung, ob alle aufsichtsrechtlichen Bedingungen erfüllt sind
  - Ermittlung und Bewertung der relevanten Risiken
  - Überprüfung der Geeignetheit des Dienstleisters
  - etc,.

Management des IKT-Drittparteienrisikos

- Wesentliche Vertragsbestimmungen ua.:
  - Klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen
  - Angabe der Standorte (Regionen oder Länder), wo die vergebenen Funktionen und IKT-Dienstleistungen erbracht werden
  - Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz
  - Verpflichtung des IKT-Drittdienstleisters bei einem IKT-Vorfall Unterstützung zu leisten
  - uneingeschränkte Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens und der zuständigen Behörde
  - Kündigungsfristen und Berichtspflichten des IKT-Drittdienstleisters
  - IKT-Drittdienstleister hat Notfallpläne zu implementieren und zu testen und über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit zu verfügen
  - Ausstiegsstrategien inklusive angemessenen Übergangszeitraum
  - Etc.

DORA - DIGITAL OPERATIONAL RESILIENCE ACT

Vorortprüfungen:

- Ab 3. Quartal VOP DORA als Prüfmodul
- Basis für die Einhaltung der DORA-VO ist ein solider und dokumentierter IKT-Risikomanagementrahmen
  - Risikoanalyse u. –bewertung
  - Business Continuity Management / Business Impact Analyse
- Richtlinien
- Prozessbeschreibungen
- Ausführliche Dokumentation

Weiterführende Informationen:

DORA – Digitale operationale Resilienz im Finanzsektor - FMA Österreich

Bei Fragen: DORA@fma.gv.at

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz