Ihr Ansprechpartner:
Ass. Thomas Teschner
E-Mail:
thomas.teschner@saarland.ihk.de
Tel.:
(0681) 9520-200
Fax:
(0681) 9520-690

GEWERBERECHT – G17

Stand: März 2025

Finanzunternehmen und IKT-Dienstleister: neue Cyberabwehr-Pflichten nach „Dora“

Mit dem **Digital Operational Resilience Act**, kurz **Dora**, schafft die EU neue Verpflichtungen für das Management von Risiken bei Cybersicherheit sowie Informations- und Kommunikationstechnologien (IKT) im Finanzsektor. Betroffen sind nicht nur nahezu alle Finanzunternehmen, sondern auch IKT-Dienstleister.

In Kraft getreten ist Dora (nachzulesen unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554) bereits im Januar 2023. National umgesetzt wurde die Dora-Verordnung mit dem Finanzmarktdigitalisierungsgesetz (FinmadiG), das am 27. Dezember 2024 im Bundesgesetzblatt verkündet worden ist. **Dora findet seit dem 17. Januar 2025 Anwendung**.

Versicherungsvermittler und -berater

Auch **Versicherungsvermittler und -berater** müssen die neuen Vorschriften beachten. Allerdings **nur, wenn** sie 250 oder mehr Personen beschäftigen und einen Jahresumsatz von mehr als 50 Millionen Euro oder eine Jahresbilanzsumme von mehr als 43 Millionen Euro aufweisen. Bei der Anwendung der Schwellenwerte ist ausschließlich auf die Umsätze aus Tätigkeiten, die der Dora-Verordnung (EU) 2022/2554 unterliegen, abzustellen.

Regelmäßige Risikokontrollen

Zentrales Element von Dora ist die regelmäßige Evaluierung der Abwehrbereitschaft gegen Cyberrisiken. Mithilfe von Schwachstellenbewertungen und -scans, Penetrationstests, Netzsicherheitsbewertungen, Open-Source-Analysen, Überprüfungen der physischen Sicherheit, Scans von Softwareprodukten, wenn möglich Quellcodeüberprüfungen, Kompatibilitäts- und Leistungstests sowie End-to-End-Tests müssen kritische IKT-Systeme künftig mindestens einmal jährlich auf Einfallstore für Cyberangriffe überprüft werden.

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland · 66104 Saarbrücken · Büroanschrift: Franz-Josef-Röder-Straße 9 · 66119 Saarbrücken
Tel. 06 81/95 20-0 · Fax 06 81/95 20-888 · E-Mail: info@saarland.ihk.de · Internet: www.saarland.ihk.de

Vornehmen sollen die Prüfungen **externe Dienstleister**, die im Bereich Penetrationstests besonders akkreditiert und zertifiziert werden, über technische und organisatorische Fähigkeiten verfügen und spezifische Fachkenntnisse in den Bereichen Bedrohungsanalyse, Penetrationstests und Red-Team-Tests nachweisen können. Lediglich **im Ausnahmefall** und nur wenn spezifische Bedingungen eingehalten werden, können **interne Tester** zum Einsatz kommen. Diese müssen aber durch die europäischen Aufsichtsbehörden EBA, ESMA oder EIOPA (je nachdem, für welche Branche der IKT-Drittdienstleister schwerpunktmäßig tätig ist) zugelassen werden. Es gilt dabei auch, Interessenkonflikte durch Design und Ausführung der Tests auszuschließen. Die für den Test erforderlichen Bedrohungsinformationen müssen darüber hinaus von einem unabhängigen dritten Unternehmen stammen.

Umfangreiche Meldepflichten

Zudem vereinheitlicht Dora die **Meldepflichten bei schwerwiegenden IKT-Vorfällen** und weitet diese auf den gesamten Finanzsektor aus. So werden Finanzunternehmen verpflichtet, einen Managementprozess zur Überwachung und Protokollierung IKT-bezogener Sicherheitsvorfälle einzurichten. Schwerwiegende Vorfälle müssen den Finanzaufsichtsbehörden gemeldet werden. Zusätzlich können Finanzinstitute sich bei erkannten Cyberbedrohungen freiwillig an die Aufsicht wenden.

Auch externe Dienstleister betroffen

Grundsätzlich **gilt Dora für** alle Banken und Kreditinstitute, Versicherungs- und Rückversicherungsunternehmen, Investmentfirmen, Zentralverwahrer, Dienstleister für Krypto-Assets, Zahlungsdienstleister und elektronische Zahlungsanbieter, Kreditratingunternehmen, Kapitalverwaltungsunternehmen, Dienstleister im Bereich des Crowdfunding, Entwickler von Banking-Apps, Hersteller von Geldautomaten sowie für weitere Unternehmen wie Transaktions- und Verbriefungsregister, Handelsplätze und Datenbereitstellungsdienste – in der Summe als "Finanzunternehmen" definiert.

Ausgenommen sind einzelne Unternehmensgruppen wie Verwalter alternativer Investmentfonds und Einrichtungen der betrieblichen Altersversorgung, Versicherungsvermittler in Nebentätigkeit sowie kleine Versicherungsvermittler und Rückversicherungsvermittler und kleine Unternehmen mit kumulativ weniger als zehn Mitarbeitern beziehungsweise unter zehn Millionen Euro Bilanzsumme.

Des Weiteren gilt Dora nicht für Hardwarehersteller, allgemeine oder elektronische Kommunikationsdienste, wohl aber für externe IKT-Anbieter, die digitale Dienste und Datendienste erbringen, einschließlich Anbietern von Cloud-Computing-Diensten, Software, Datenanalysediensten und Rechenzentren. Finanzinstitute sind mit der neuen Verordnung verpflichtet, ein **Verzeichnis ihrer IKT-Verträge mit Dritten zu führen (Informationsregister)** und den Aufsichtsbehörden auf Verlangen vorzulegen. Außerdem müssen sie die IKT-Dienstleister vor Vertragsabschluss sorgfältig prüfen.

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland · 66104 Saarbrücken · Büroanschrift: Franz-Josef-Röder-Straße 9 · 66119 Saarbrücken
Tel. 06 81/95 20-0 · Fax 06 81/95 20-888 · E-Mail: info@saarland.ihk.de · Internet: www.saarland.ihk.de

Bis zum **11. April 2025** müssen Finanzunternehmen unter DORA ihr **Informationsregister bei der BaFin einreichen**. Die Abgabe der Informationsregister erfolgt über das Fachverfahren „Digital Operationale Resilience Act (DORA)“ in der Melde- und Veröffentlichungsplattform (MVP) der BaFin. Finanzunternehmen können ihre Informationsregister in zwei Formaten über die MVP an die BaFin übermitteln. Nähere Infos stellt die BaFin hier zur Verfügung: https://www.bafin.de/DE/Aufsicht/DORA/Informationsregister_und_Anzeigepflichten/Informationsregister_und_Anzeigepflichten_node.html

Gemäß Dora müssen die Drittanbieter zudem bestimmte IT-Sicherheitsstandards einhalten – und die Verträge haben Kündigungsmöglichkeiten für bestimmte Szenarien zu enthalten. Werden kritische oder wichtige Funktionen von den Finanzinstituten outgesourct, kommen zusätzliche Pflichten hinzu. Die Aufsichtsbehörden werden ermächtigt, weitere Vorgaben einschließlich technischer Standards für solche Verträge zu definieren.

Identifikation von IKT-Dienstleistern

Finanzunternehmen und Versicherungen müssen die Eignung von IKT-Dienstleistern vor Vertragsabschluss prüfen und die Einhaltung bestimmter Qualitäts- und Sicherheitsstandards kontinuierlich überwachen. Im „Final Report on Draft ITS on Register of Information” ist unter anderem festgelegt, wie Institute und Unternehmen des europäischen Finanzsektors ihre vertraglichen Vereinbarungen mit IKT-Drittanbietern dokumentieren und überwachen müssen.

Um diese Vorgaben umzusetzen, ist eine klare und standardisierte Identifikation von IKT-Dienstleistern unerlässlich. Die Identifikation kann über zwei unterschiedliche Identnummern erfolgen:

Die **EUID**-Nummer (European Unified ID) wird i.d.R. automatisch angelegt. Dabei werden die Daten werden aus den nationalen Unternehmensregistern in das Europäische Unternehmensregister eingespielt. Unternehmer können hier prüfen, ob und über welche EUID sie verfügen: https://euid.eu/

Die **LEI**-Nummer (Legal Entity Identifier) kann hier beantragt werden: https://www.leireg.de/de/. IKT-Dienstleister, die bereits über eine EUID verfügen, können diese verwenden und müssen nicht zusätzlich eine LEI beantragen. Das ergibt sich aus Artikel 3 Punkt 6 der Durchführungsverordnung 2024/2956. Sofern sie jedoch auch über eine aktive LEI verfügen, sind beide Nummern - EUID und LEI - anzugeben.

Wo finde ich weitere Informationen zu Dora?

Umfangreiche und aktuelle Informationen zu Dora bietet die Bundesanstalt für Finanzdienstleistungsaufsicht unter https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html Ausführlich wird dort auch über die Erstellung des Informationsregisters informiert und Vorlagen angeboten.

Dieses Merkblatt soll – als Service Ihrer IHK – nur erste Hinweise geben und erhebt daher keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland · 66104 Saarbrücken · Büroanschrift: Franz-Josef-Röder-Straße 9 · 66119 Saarbrücken
Tel. 06 81/95 20-0 · Fax 06 81/95 20-888 · E-Mail: info@saarland.ihk.de · Internet: www.saarland.ihk.de