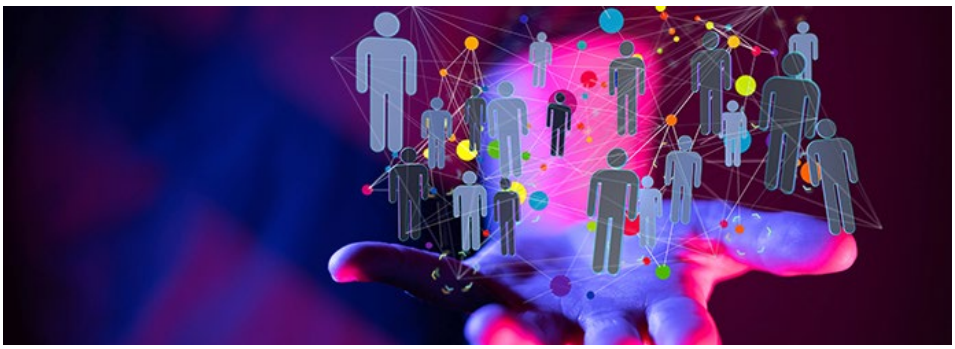
Die neuen Vorschriften zur Untervergabe von IT-Services unter DORA

Die Durchführungsverordnung (EU) 2025/532 der Europäischen Kommission ist am 22. Juli 2025 in Kraft getreten. Sie präzisiert, welche Aspekte Finanzinstitute in Bezug auf den Einsatz von Subunternehmern durch ihre IT-Dienstleister, deren Leistungen kritische oder wichtige Funktionen eines Finanzinstituts unterstützen, zu berücksichtigen und bewerten haben. Zwecks Umsetzung ist eine sorgfältige Überarbeitung von Verträgen zwischen Finanzinstituten und ihren IT-Dienstleistern sowie zwischen IT-Dienstleistern und ihren Subunternehmern erforderlich. Dies gilt auch für Verträge mit IT-Dienstleistern oder Subunternehmern außerhalb der EU.



© IMAGO / Wirestock

Identifizierung, Überwachung, Prüfung: Finanzinstitute müssen auch beim Einsatz von IT-Dienstleistern und deren Subunternehmern Herr der Lage bleiben.

Der sogenannte Digital Operational Resilience Act (Verordnung (EU) 2022/2554 – DORA) bezweckt, die Widerstandfähigkeit von EU-Finanzinstituten gegenüber IT-Störungen, Cyberangriffen und anderen digitalen Risiken zu stärken. Neben Anforderungen an das IT-Risikomanagement, das Melden von IT-Vorfällen und das Testen der operativen Resilienz enthält DORA Anforderungen, die das Outsourcing von IT-Services durch Finanzinstitute an Dritte, einschließlich des Einsatzes von Subunternehmern durch solche Dritte, betreffen. Die Europäischen Aufsichtsbehörden (ESAs) haben die DORA-Anforderungen an den Einsatz von Subunternehmern durch IT-Dienstleister in sogenannten technischen Regulierungsstandards (RTS) präzisiert, welche die Kommission am 24. März 2025 angenommen und am 2. Juli 2025 als Durchführungsverordnung (EU) 2025/532 im Amtsblatt der Europäischen Union veröffentlicht hat. Am 22. Juli 2025 ist die Durchführungsverordnung in Kraft getreten (Subunternehmer-RTS).

Die Anforderungen an den Einsatz von Subunternehmern durch IT-Dienstleister von Finanzinstituten umfassen:

Due Diligence: Vor Abschluss eines Vertrags mit einem IT-Dienstleister müssen Finanzinstitute eine umfassende Risikoabwägung durchführen und unter anderem Risiken bewerten, die sich aus etwaig geplantem Einsatz von Subunternehmern durch den IT-Dienstleister ergeben (Art. 28 Abs. 4 DORA und Art. 3 Subunternehmer-RTS).

Identifizierung der Kette von Subunternehmern: Finanzinstitute haben umfassende Informationen über die Kette von Subunternehmern zu erfragen und insbesondere die gesamte Kette von Subunternehmern zu identifizieren, deren Leistungen kritische oder wichtige Funktionen des Finanzinstituts oder wesentliche Teile davon unterstützen (ErwG 1 Subunternehmer-RTS). Bereits vor Abschluss eines Vertrags mit einem IT-Dienstleister müssen Finanzinstitute prüfen, ob dieser in der Lage ist, seine Subunternehmer zu identifizieren (Art. 3 lit. b Subunternehmer-RTS). Finanzinstitute haben alle Subunternehmer ihrer IT-Dienstleister, deren Leistungen kritische oder wichtige Funktionen des Finanzinstituts oder wesentliche Teile davon betreffen, in einem Informationsregister aufzuführen (Art. 3 Abs. 6 Durchführungsverordnung (EU) 2024/2956), das zuständigen Behörden auf Anfrage zur Verfügung zu stellen ist (Art. 28 Abs. 3 DORA). Zudem müssen Verträge zwischen Finanzinstituten und IT-Dienstleistern vorsehen, dass das Finanzinstitut über wesentliche Änderungen im Zusammenhang mit Subunternehmern informiert wird (Art. 5 Abs. 1 Subunternehmer-RTS).

Überwachung: Finanzinstitute müssen die Auswirkungen potenziell langer oder komplexer Ketten von Subunternehmern auf ihre Fähigkeit, die bezogenen IT-Services vollständig zu überwachen, sowie auf die Fähigkeit der zuständigen Behörde, das Finanzinstitut wirksam zu beaufsichtigen, bewerten (Art. 29 Abs. 2 DORA und Art. 1 lit. d Subunternehmer-RTS). Finanzinstitute müssen ihre IT-Dienstleister vertraglich verpflichten, ihre Subunternehmer, die kritische oder wichtige Funktionen des Finanzinstituts oder wesentliche Teile davon unterstützen, zu überwachen und dem Finanzinstitut Bericht zu erstatten.

Zugangs- und Prüfrechte: Finanzinstitute müssen sich uneingeschränkte Zugangs- und Prüfrechte – einschließlich Zugang zu Unterlagen – gegenüber ihren IT-Dienstleistern und deren Subunternehmern einräumen lassen (Art. 30 Abs. 3 lit. e DORA und Art. 4 Abs. 1 lit. j Subunternehmer-RTS).

Sonstige Anforderungen an den Einsatz von Subunternehmern: Verträge zwischen Finanzinstituten und IT-Dienstleistern haben verschiedene weitere zwingende Inhalte in Bezug auf den Einsatz von Subunternehmern zu enthalten, die in Art. 30 DORA und Art. 4 und 6 Subunternehmer-RTS festgelegt sind, etwa, dass IT-Dienstleister für die Leistungserbringung durch ihre Subunternehmer verantwortlich sind, an welchen Orten Subunternehmer Daten verarbeiten oder speichern oder, dass vertragliche Anforderungen an Geschäftskontinuität, IT-Sicherheit, Notfallpläne und Leistungsgüte an Subunternehmer weiterzureichen sind.

Bevor die Kommission das Subcontracting-RTS am 24. März 2025 angenommen hat, hatte sie einen früheren Entwurf vom 26. Juli 2024 in einem Schreiben vom 21. Januar 2025 abgelehnt, da Bestimmungen in Art. 5 des Entwurfs im Zusammenhang mit der Kette von Subunternehmern über die in DORA vorgesehene Ermächtigung der ESAs hinausgehen würden. Die ESAs haben am 7. März 2025 zugestimmt, Art. 5 des Entwurfs zu streichen. Auch soweit dies formale Anforderungen in Bezug auf die Kette von Subunternehmern verringert, bleiben wesentliche Anforderungen an die Identifizierung und Überwachung der Kette von Subunternehmern bestehen.

Jan Pohle und Verena Reichstein

© Dentons

Jan Pohle ist Partner im Düsseldorfer Büro von Dentons und Mitglied der Praxisgruppe Intellectual Property and Technology. Im Segment Technologie- und Datenschutzrecht verfügt er über mehr als zwanzig Jahre Berufserfahrung. Er berät nationale und internationale Unternehmen zu komplexen, technologiebezogenen Projekten.

© Dentons

Verena Reichstein ist Senior Associate im Düsseldorfer Büro von Dentons und Mitglied der Praxisgruppe Intellectual Property and Technology. Sie ist spezialisiert auf die Beratung national und international agierender Unternehmen zu Rechtsfragen des Informationstechnologierechts.