Autor:

Dr. Lukas Fleischer
Associate

04.04.2025

IKT-Drittdienstleister unter der DORA: Vertragsgestaltung im Lichte digitaler Resilienz

Kurz gelesen:

Ab dem 17. Januar 2025 gilt der Digital Operational Resilience Act („DORA“) EU-weit. Der DORA schafft einen umfassenden Rechtsrahmen, der darauf abzielt, die digitale Resilienz von Finanzunternehmen zu stärken. Der DORA verpflichtet Finanzunternehmen (u.a.) dazu, mit deren Dienstleistern im Bereich Informations- und Kommunikationstechnologie (sog. IKT-Drittdienstleister, z.B. Softwareanbieter) spezifische vertragliche Regelungen zu vereinbaren. Was dies für Dienstleister von Finanzunternehmen bedeuten kann, beleuchtet der folgende Beitrag.

1. IKT-Drittdienstleister

Der DORA gilt primär für Finanzunternehmen, wie etwa Kredit- und Zahlungsinstituten sowie für Versicherungsunternehmen (Art. 2 Abs. 1 und 2 DORA). An die Ausgestaltung der digitalen Systeme und Prozesse dieser Unternehmen stellt der DORA spezifische Anforderungen. Dazu gehört neben der Bewertung digitaler Risiken (z.B. Cyberattacken) insbesondere auch die Implementierung von Risikominderungsmaßnahmen.

Neben Finanzunternehmen gilt der DORA auch für sog. IKT-Drittdienstleister (§ 2 Abs. 1 Buchst. u DORA). Der Begriff des IKT-Drittdienstleisters ist sehr weit formuliert und zielt darauf ab, die an der digitalen Transformation der Finanzdienstleistungsbranche Beteiligten den Regelungen des DORA zu unterwerfen. Begrifflich umfasst sollen daher im Grundsatz sämtliche Unternehmen sein, die fortlaufend digitale Dienste oder Datendienste über IKT-Systeme an einen oder mehrere interne oder externe Nutzer in der Finanzbranche bereitstellen (ErwGr. 35 zur DORA), also üblicherweise insb.:

- **Cloud-Computing-Anbieter:** Unternehmen, die Speicher- und Rechenressourcen über das Internet bereitstellen.
- **Softwareanbieter:** Unternehmen, die Softwarelösungen für Finanzunternehmen entwickeln oder bereitstellen.
- **Datenanalysedienste:** Unternehmen, die Datenverarbeitung und -analyse für Finanzinstitute durchführen.
- **Rechenzentren:** Unternehmen, die physische Infrastruktur für die Speicherung und Verarbeitung von Daten anbieten.

2. Vertragsinhalte nach Art. 30 DORA

Für Finanzunternehmen enthält der DORA besondere Pflichten, welche für die Zusammenarbeit mit bzw. die Beauftragung von Drittdienstleistern zu beachten sind. Eine zentrale Aufgabe des handelnden Finanzunternehmens ist dabei die Ausarbeitung einer vertraglichen Vereinbarung mit dem beauftragten IKT-Drittdienstleister (Art. 30 DORA). Das Finanzunternehmen muss sicherstellen, dass die Rechte und Pflichten beider Parteien klar definiert und schriftlich festgehalten werden (Art. 30 Abs. 1 DORA).

Für die Ausgestaltung der vertraglichen Vereinbarung enthält Art. 30 Abs. 2 DORA **Mindestregelungsinhalte**, die bei jeder Beauftragung eines IKT-Drittdienstleisters durch das Finanzunternehmen umzusetzen sind. Dazu gehören insb.:

- **Leistungsbeschreibung**: Eine klare Definition der IKT-Dienstleistungen (einschließlich der Bedingungen für Unteraufträge).
- **Datenschutz**: Bestimmungen zur Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit auf den Datenschutz (einschließlich des Schutzes personenbezogener Daten).
- **Unterstützung und Zusammenarbeit**: Die Verpflichtung des IKT-Drittdienstleisters, das Finanzunternehmen bei einem IKT-Vorfall, der mit dem IKT-Dienst des IKT-Drittdienstleisters in Verbindung steht, zu unterstützen. Die Verpflichtung des IKT-Drittdienstleisters, mit den für das Finanzunternehmen zuständigen Aufsichtsbehörden zu kooperieren.
- **Beendigungsklauseln**: Kündigungsrechte und Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen.

Sofern der beauftragte IKT-Drittdienstleister das Finanzunternehmen bei **kritischen oder wichtigen Funktionen** unterstützt, sind über die Mindestregelungsinhalte zusätzliche Regelungen in der Vertragsvereinbarung aufzunehmen (Art. 30 Abs. 3 DORA). Eine Funktion ist kritisch oder wichtig, wenn deren Ausfall beispielsweise die **finanzielle Leistungsfähigkeit** des Finanzunternehmens oder dessen **Geschäftsbetrieb erheblich beeinträchtigt**. Sofern eine kritische oder wichtige Funktion gegeben ist, sind zusätzlich insb. die folgenden Vertragsinhalte zu regeln:

- **IKT-Sicherheit**: Die Verpflichtung des IKT-Drittdienstleisters Notfallpläne zu implementieren und zu testen. Die Pflicht des IKT-Drittdienstleisters Maßnahmen, Tools sowie Leit- und Richtlinien zur IKT-Sicherheit auszuarbeiten und zu pflegen.
- **Penetrationstests**: Die Pflicht des IKT-Drittdienstleisters das Finanzunternehmen bei sog. Threat-Led-Penetration-Tests (TLPTs) zu unterstützen.
- **Überwachungs- und Zugangsrechte**: Das Recht des Finanzunternehmens und der zuständigen Behörde uneingeschränkten Zugang zu den Geschäftsräumen des IKT-Drittdienstleisters zu erhalten, um Inspektionen und Audits durchzuführen.
- **Ausstiegsstrategie:** Regelungen zur Gewährleistung der Geschäftskontinuität im Falle einer Vertragsbeendigung oder eines Wechsels des IKT-Drittdienstleisters.

3. To-Dos for Businesses

Da sich Art. 30 DORA unmittelbar nur an Finanzunternehmen richtet, folgt daraus für IKT-Drittdienstleister zwar nicht automatisch eine Pflicht zur Überarbeitung bestehender (Dienstleistungs-)Verträge. Jedoch sollten sich IKT-Drittdienstleister darauf vorbereiten, dass ihre Kunden aus dem Finanzbereich (Finanzunternehmen) sie mit der Umsetzung der in der DORA festgelegten Regelungen konfrontieren. Demnach sind Unternehmen, die Dienstleistungen für Finanzunternehmen bereitstellen, gut beraten, sich folgende **vertragsrechtliche Fragen** zu stellen:

- Fällt das Unternehmen als Dienstleister mit der angebotenen Dienstleistung unter den Begriff des IKT-Drittdienstleisters?
- Welche Art eines IKT-Dienstes erbringt das Unternehmen? Unterstützt das Unternehmen eine wichtige oder kritische Funktion des Finanzunternehmens oder betrifft die Dienstleistung lediglich eine „unkritische“ Funktion beim Finanzunternehmen?
- Entsprechen die bestehenden Vertragswerke den rechtlichen Anforderungen, welche die DORA an den zu erbringenden IKT-Dienst stellt?
- Welche vertraglichen Regelungen sind mit den eigenen (Unter-)Auftragsverarbeitern abzuschließen, um ein Haftungsrisiko gegenüber dem beauftragenden Finanzunternehmen zu vermeiden?