Vertragsinhalte für IKT-Verträge

- Ein Cheatsheet aus der DORA-Werkstatt -

DISCLAIMER: Das Cheatsheet dient als Orientierungshilfe für die erste Einschätzung, welche Vertragsinhalte in IKT-Verträge unter Berücksichtigung der Vorgaben nach AT 9 Tz. 7 MaRisk sowie gemäß DORA-Verordnung aufgenommen werden müssen. Das Cheatsheet ist nicht rechtsverbindlich und ersetzt keine juristische Prüfung.

IKT-Verträge zwischen Finanzinstituten und ihren IKT-Dienstleistern müssen je nach Relevanz den Anforderungen des Digital Operational Resilience Act (DORA) und/oder den Mindestanforderungen an das Risikomanagement (MaRisk) entsprechen. Dieses Cheatsheet bietet einen Ordnungsrahmen zur Systematisierung von IKT-Verträgen in die Kategorien **Baseline Services, Core Services, Hidden Giants und Business Backbone**.

Baseline Services: Verträge in diesem Quadranten betreffen IKT-Dienstleistungen, die weder für die Finanzstabilität noch für die tägliche Funktionsfähigkeit des Unternehmsens von zentraler Bedeutung sind. Sie werden weder als wesentliche Auslagerungen gemäß MaRisk betrachtet noch haben sie eine Relevanz für kritische oder wichtige Funktionen nach DORA. Die Risiken, die mit solchen IKT-Verträgen verbunden sind, sind vergleichsweise gering, weshalb auch die Anforderungen an die Verträge weniger anspruchsvoll sind. Im Vergleich zur bisherigen MaRisk- und BAIT-Welt gibt es gemäß Art. 30 Abs. 2 DORA auch für diese „Baseline Services“ Mindestvertragsinhalte , die erfüllt werden müssen.

Core Services: Diese IKT-Dienstleistungen sind gemäß MaRisk als wesentliche Auslagerungen einzustufen, haben jedoch keine Relevanz für die kritischen oder wichtigen Funktionen nach DORA. Daher müssen die entsprechenden IKT-Verträge die Mindestanforderungen gemäß AT 9 Tz. 7 MaRisk erfüllen sowie die allgemeinen Anforderungen an IKT-Dienstleistungen gemäß Art. 30 Abs. 2 DORA.

Hidden Giants: IKT-Verträge, die in diesem Quadranten liegen, gelten gemäß DORA als kritisch oder wichtig, werden jedoch nicht als wesentliche Auslagerungen nach MaRisk eingestuft. Ob eine solche Konstellation in der Praxis häufig vorkommt, ist fraglich, da die Relevanz für kritische oder wichtige Funktionen häufig auch die Einstufung als wesentliche Auslagerung nach MaRisk beeinflusst. Dennoch müssen diese IKT-Verträge „lediglich“ die Mindestvertragsinhalte für kwF-relevante IKT-Dienstleistungen gemäß Art. 30 Abs. 2 und Abs. 3 DORA enthalten.

Business Backbone: Diese IKT-Dienstleistungen sind sowohl nach DORA als auch nach MaRisk von höchster Bedeutung. Sie erfordern strenge vertragliche Vereinbarungen sowie eine kontinuierliche Überwachung und Steuerung der IKT-Dienstleister. Für diese Dienstleistungen müssen sowohl die Mindestvertragsinhalte für wesentliche Auslagerungen gemäß AT 9 Tz. 7 MaRisk als auch die Anforderungen gemäß Art. 30 Abs. 2 und Abs. 3 DORA für kwF-relevante IKT-Dienstleistungen erfüllt werden.

Vorgehen:

Die Anforderungen an die jeweiligen IKT-Verträge wurden durch eine gründliche Analyse von AT 9 Tz. 7 MaRisk und der DORA-VO ermittelt. Dabei wurden neben den in Art. 30 Abs. 2 und Abs. 3 DORA festgelegten Mindestanforderungen auch weitere relevante Stellen in verschiedenen Artikeln der DORA-VO entdeckt, die zusätzliche vertragsrelevante Anforderungen enthalten.

Alle identifizierten Vertragsanforderungen wurden auf semantische Übereinstimmungen hin geprüft und gegebenenfalls zusammengeführt. So wurden Redundanzen aus der Überschneidung von MaRisk- und DORA-Vorgaben entfernt und eine klare, konsolidierte Anforderungsliste erstellt.

Angesichts der Vielzahl an Anforderungen wurden diese in 8 thematische Kategorien unterteilt, um eine klare, praxisorientierte und leicht verständliche Struktur zu erreichen:

A. Allgemeine Vertragsbestimmungen
B. Bestimmungen zur IKT-Dienstleistung
C. Bestimmungen zum Management von Unterauftragnehmern
D. Bestimmungen zum IKT-Risikomanagementrahmen
E. Bestimmungen zum IKT-BCM und Management von IKT-Vorfällen
F. Bestimmungen zu Kündigung und Exit
G. Bestimmungen zur Prüfung und Überwachung
H. Bestimmungen zum Berichtswese

Hinweis: Die identifizierten Anforderungen wurden mit der Aufsichtsmitteilung der Bafin zu den Mindestvertragsinhalten DORA (Stand Juni 2024) abgeglichen und beinhalten darüber hinaus auch die Anforderungen aus dem RTS Subcontracting (Stand 24.03.2025).

A: Allgemeine Vertrags-bestimmungen	B: Bestimmungen zur IKT-Dienstleistung	C: Bestimmungen zum Management von Unterauftragnehmern	D: Bestimmungen zum IKT-Risikomanagement-rahmen	E: Bestimmungen zum IKT-BCM und Management von IKT-Vorfällen	F: Bestimmungen zu Kündigung und Exit	G: Bestimmungen zur Prüfung und Überwachung	H: Bestimmungen zum Berichtswesen
A.1 - Schriftform der vertraglichen Vereinbarungen	B.1 - Beschreibung der IKT-Dienstleistung	C.1 - Regelungen zur Unterauftragsvergabe und Weiterverlagerung	D.1 - Festlegungen zu Datenschutz und Schutz personenbezogener Daten	E.1 - Unterstützung bei IKT-Vorfällen	F.1 - Regelungen zur Wiederherstellung und Rückgabe von Daten im Exit-Fall	G.1 - Zusammenarbeit mit Behörden	H.1 - Vereinbarung zu Berichtspflichten bei Beeinträchtigung des Leistungsniveaus
alle	alle	🏛 + 🏦 + 🏢	alle	alle	alle	alle	🏛 + 🏦 + 🏢
A.2 - Zuweisung der Rechte, Pflichten und Verantwortlichkeiten	B.2 - Festlegung der Standorte für die Erbringung von IKT-Dienstleistungen	C.2 - Nachbildung relevanter Vertragsinhalte bei Unteraufträgen	D.2 - Festlegungen zu Informationssicherheit und Schutz von Informationen	E.2 - Regelung der Vergütung für Unterstützung bei IKT-Vorfällen	F.2 - Zugang und Zugriff zu Daten und Räumlichkeiten im Exit-Fall	G.2 - Zugangs-bestimmungen	H.2 - Vereinbarung zur Bereitstellung von Berichten über die Erbringung der IKT-Dienstleistungen
alle	alle	🏛 + 🏦 + 🏢	alle	alle	alle	🏛 + 🏦 + 🏢	🏛 + 🏦 (nur kwF)
A.3 - Verfahren zur Verlängerung der vertraglichen Vereinbarungen	B.3 - Festlegung des Ortes der Datenverarbeitung und -speicherung	C.3 - Anforderungen an das Management des IKT-Drittparteienrisikos	D.3 – Teilnahme-bedingungen an Schulungsprogrammen	E.3 - Vorgaben für Wiederherstellungszeit und -punkte	F.3 - Allgemeine Kündigungsrechte und Mindest-kündigungsfristen	G.3 - Recht auf fortlaufende Überwachung der IKT-Dienstleistung	H.3 - Vereinbarung zur Bereitstellung von Berichten über Maßnahmen und Tests zur Geschäftsfortführung
🏛 + 🏦 (nur kwF)	alle	🏛 + 🏦 (nur kwF)	🏛 + 🏦 + 〓	Alle BCM-relevanten	alle	🏛 + 🏦 + 🏢	🏛 + 🏦 (nur kwF)
A.4 - Vereinbarung des Beginns und Endes der Vereinbarung	B.4 - Benachrichtigung bei Änderungen der Standorte	C.4 - Überwachungs- und Berichtspflichten des IKT-Dienstleisters	D.4 - Anforderungen an die Daten- und Systemsicherheit	E.4 - Meldung von IKT-Vorfällen durch den IKT-Dienstleister	F.4 - Kündigungsrechte bei Verstößen und Risiken des IKT-Dienstleisters	G.4 - Uneingeschränkte Zugangs-, Inspektions- und Auditrechte	H.4 - Vereinbarung zur Bereitstellung von Berichten über IKT-Sicherheit
🏢 + 🏦 (nur AT 9)	alle	🏛 + 🏦 (nur kwF)	🏛 + 🏦 + 〓	🏛 + 🏦 (nur kwF)	alle	🏛 + 🏦 + 🏢	🏛 + 🏦 (nur kwF)
A.5 - Festlegung des geltenden Rechts für die Vereinbarung	B.5 - Beschreibung der Dienstleistungsgüte und regelmäßige Aktualisierungen	C.15 - Überwachungs- und Bericht-erstattungspflichten der Unterauftragnehmer	D.5 - Anforderungen an die Netzwerksicherheit	E.5 - Meldung schwerwiegender zahlungsbezogener Vorfälle	F.5 - Unterstützung bei der Übertragung oder Reintegration der ausgelagerten Aktivitäten	G.5 - Vereinbarung über Umfang, Häufigkeit und Verfahren der Audits und Inspektionen	H.5 - Vereinbarungen zur Bereitstellung von Audit-Berichten und Zertifizierungen
🏢 + 🏦 (nur AT 9)	alle	🏛 + 🏦 (nur kwF)	🏛 + 🏦 + 〓	🏛 + 🏦 (nur kwF)	🏢 + 🏦 (nur AT 9)	🏛 + 🏦 + 🏢	🏛 + 🏦 (nur kwF)
A.6 - Versicherungsnachweis für bestimmte Risiken	B.6 - Vollständige Beschreibung der Dienstleistungsgüte inklusive präziser Leistungsziele	C.6 - Zugangs-, Inspektions- und Auditrechte bei Unterauftragnehmern	D.6 - Spezifikation Sicherheitsmaßnahmen für Network Services Agreements:	E.6 - Anforderungen an die Umsetzung und Überprüfung eines Notfallkonzeptes	F.6 - Kündigungsrechte bei Verstößen und Risiken in Zusammenhang mit Unterauftragnehmern	G.6 - Recht auf Zugang zu Informationen	H.6 - Vereinbarungen über die Bereitstellung von Berichten der Unterauftragnehmer
🏢 + 🏦 (nur AT 9)	🏛 + 🏦 + 🏢	🏛 + 🏦 (nur kwF)	🏛 + 🏦 + 〓	🏢 + 🏦 (nur AT 9)	🏛 + 🏦 (nur kwF)	🏛 + 🏦 + 🏢	🏛 + 🏦 (nur kwF)
	B.7 - Festlegung von Leistungsindikatoren und Maßnahmen zur Überwachung der Leistungsfähigkeit	C.7 - IKT-Sicherheitsstandards und Notfallpläne bei Unterauftragnehmern	D.7 - Anforderungen an IKT-Sicherheitsmaßnahmen, Tools und Richtlinien	E.7 - Implementierung und Test von Notfallplänen durch den IKT-Drittdienstleister	F.7 - Vereinbarung einer Ausstiegsstrategie	G.7 - Recht auf Anfertigung von Kopien relevanter Unterlagen	H.7 - Meldung von und Berichte zu IKT-Vorfällen durch den IKT-Dienstleister
	🏛 + 🏦 (nur kwF)	🏛 + 🏦 (nur kwF)	🏛 + 🏦 (nur kwF)	🏛 + 🏦 (nur kwF)	🏛 + 🏦 (nur kwF)	🏛 + 🏦 (nur kwF)	🏛 + 🏦 (nur kwF)

A: Allgemeine Vertrags-bestimmungen	B: Bestimmungen zur IKT-Dienstleistung	C: Bestimmungen zum Management von Unterauftragnehmern	D: Bestimmungen zum IKT-Risikomanagement-rahmen	E: Bestimmungen zum IKT-BCM und Management von IKT-Vorfällen	F: Bestimmungen zu Kündigung und Exit	G: Bestimmungen zur Prüfung und Überwachung	H: Bestimmungen zum Berichtswesen
	B.8 - Festlegung von Konformitätsindikatoren und Maßnahmen zur Überwachung der Konformität	C.8 - Überwachung von Unterauftragnehmern durch den IKT-Drittdienstleister	D.8 - Anforderungen an das IKT-Risikomanagement	E.8 - Vereinbarungen zur Unterstützung des IKT-Drittdienstleisters beim Testen von IKT-Geschäftsfort-führungsplänen	F.8 - Festlegung eines Übergangszeitraums in der Ausstiegsstrategie	G.8 - Vereinbarungen zur Durchführung von unabhängigen Überprüfungen und Audits	
	🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)	
	B.9 - Festlegung von Maßnahmen bei Nichteinhaltung der Dienstleistungs-vereinbarungen	C.9 - Sicherstellung der Kontinuität der IKT-Dienstleistungen entlang der Unterauftragnehmer-kette	D.9 - Anforderungen an die Bereitstellung von Informationen zu Cyberbedrohungen und Schwachstellen		F.9 - Szenarien in Ausstiegsstrategien	G.9 - Recht zur Änderung des Umfangs von Zertifizierungen und Auditberichten	
	🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)		🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)	
		C.10 - Risikobewertung von Unterauftragnehmern	D.10 - Anforderungen an Tests der digitalen operationalen Resilienz			G.10 - Recht auf Durchführung von Einzel- und Sammelaudits	
		🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)			🦣 + 🍴 (nur kwF)	
		C.11 - Anzeigepflicht von wesentlichen Änderungen der Unterauftragsvergabe	D.11 - Festlegungen zur Durchführung von IKT-Tests			G.11 - Recht auf alternative Bestätigungsniveaus bei betroffenen Kundenrechten	
		🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)			🦣 + 🍴 (nur kwF)	
		C.12 - Umsetzung von Änderungen der Unterauftrags-vereinbarungen	D.12 - Verpflichtung zur Teilnahme an TLPP			G.12 - Weisungsrechte des Finanzunternehmens	
		🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)			🕯 + 🍴 (nur AT 9)	
		C.13 - Mitteilungsfrist für Änderungen der Unterauftrags-vereinbarungen	D.13 - Optionale Vereinbarung über gebündelte TLPTs				
		🦣 + 🍴 (nur kwF)	🦣 + 🍴 (nur kwF)				
		C.14 - Ablehnung und Anpassung von Änderungen der Unterauftrags-vereinbarungen					
		🦣 + 🍴 (nur kwF)					

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
A: Allgemeine Vertragsbestimmungen						
A.1 - Schriftform der vertraglichen Vereinbarungen	Der Vertrag muss sicherstellen, dass Rechte und Pflichten der Parteien in einem schriftlichen Dokument festgehalten werden, das in Papierform oder als dauerhaft zugängliches, herunterladbares Format vorliegt. Wesentliche Änderungen und das Verfahren zur Verlängerung müssen ebenfalls schriftlich festgehalten und von allen Parteien unterzeichnet werden.	Art. 30 Abs. 1 DORA: Die Rechte und Pflichten […] werden eindeutig zugewiesen und schriftlich dargelegt. Der vollständige Vertrag [...] wird in einem schriftlichen Dokument, das den Parteien in Papierform zur Verfügung steht, oder in einem Dokument in einem anderen herunterladbaren, dauerhaften und zugänglichen Format dokumentiert. AT 9 Tz. 7 MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: [...] Art. 8 Abs. 1 RTS TPPol: In der Leitlinie wird festgelegt, dass die einschlägige vertragliche Vereinbarung schriftlich abzufassen ist [...] Art. 8 Abs. 4 RTS TPPol: Die Leitlinie stellt sicher, dass wesentliche Änderungen der vertraglichen Vereinbarung in einem schriftlichen Dokument förmlich festgehalten werden, das von allen Parteien datiert und unterzeichnet wird […]	x	x	x	x
A.2 - Zuweisung der Rechte, Pflichten und Verantwortlichkeiten	Der Vertrag muss sicherstellen, dass die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittdienstleisters eindeutig zugewiesen werden, einschließlich der Aufteilung der Aufgaben und Verantwortlichkeiten für Informationssicherheit und der Verantwortlichkeiten des IKT-Dienstleisters für Unterauftragnehmer.	Art. 30 Abs. 1 DORA: Die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittdienstleisters werden eindeutig zugewiesen [...]. Art. 30 Abs. 2 lit. a DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: a) eine klare und vollständige Beschreibung aller Funktionen [...] Art. 11 Abs. 2 lit. k (b) RTS RMF: Das [...] Verfahren für die Daten- und Systemsicherheit umfasst [...] für IKT-Assets oder -Dienstleistungen, die von einem IKT- Drittdienstleister betrieben werden, die Ermittlung und Umsetzung von [...] klare Aufteilung der die Informationssicherheit betreffenden Aufgaben und Verantwortlichkeiten zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister [...] Art. 4 lit. a RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, [...] a) dass der IKT-Drittdienstleister für die Erbringung der von den Unterauftragnehmern erbrachten Dienstleistungen verantwortlich ist;	X	X	X	X
A.3 - Verfahren zur Verlängerung der vertraglichen Vereinbarungen	Der Vertrag muss das Verfahren zur Verlängerung der vertraglichen Vereinbarungen klar festlegen. Diese Regelung muss sicherstellen, dass alle Verlängerungen ordnungsgemäß dokumentiert und von beiden Parteien datiert und unterzeichnet werden.	Art. 8 Abs. 4 RTS TPPol: Die Leitlinie stellt sicher, dass wesentliche Änderungen der vertraglichen Vereinbarung in einem schriftlichen Dokument förmlich festgehalten werden, das von allen Parteien datiert und unterzeichnet wird und in dem das Verfahren zur Verlängerung der vertraglichen Vereinbarungen festgelegt ist.			X	X
A.4 - Vereinbarung des Beginns und Endes der Vereinbarung	Der Vertrag muss das Datum des Beginns sowie gegebenenfalls das Enddatum der Auslagerungsvereinbarung festlegen, um klare zeitliche Rahmenbedingungen für die Vertragsbeziehung zu definieren.	AT 9 Tz. 7 lit. b MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: b) Datum des Beginns und ggf. des Endes der Auslagerungsvereinbarung,		X		X
A.5 - Festlegung des geltenden Rechts für die Vereinbarung	Der Vertrag muss das geltende Recht für die Auslagerungsvereinbarung festlegen, insbesondere wenn es von deutschem Recht abweicht, um Klarheit über die rechtlichen Rahmenbedingungen der Vereinbarung zu schaffen.	AT 9 Tz. 7 lit. c MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: c) sofern von deutschem Recht abweichend, das geltende Recht für die Auslagerungsvereinbarung,		X		X
A.6 - Versicherungsnachweis für bestimmte Risiken	Der Vertrag muss festlegen, dass das Auslagerungsunternehmen für bestimmte Risiken einen Versicherungsnachweis vorzulegen hat, soweit dies zutreffend ist. Dies stellt sicher, dass das Auslagerungsunternehmen für potenzielle Risiken ausreichend abgesichert ist und das Finanzunternehmen im Schadensfall geschützt wird.	AT 9 Tz. 7 lit. f MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: f) soweit zutreffend, dass das Auslagerungsunternehmen für bestimmte Risiken einen Versicherungsnachweis vorzulegen hat.		X		X
B: Bestimmungen zur IKT-Dienstleistung						
B.1 - Beschreibung der IKT-Dienstleistung	Der Vertrag muss eine klare und vollständige Beschreibung aller IKT-Dienstleistungen enthalten, die der IKT-Drittdienstleister zu erbringen hat, um sicherzustellen, dass die erwarteten Leistungen genau definiert sind.	Art. 30 Abs. 2 lit. a DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: a) eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat, […] AT 9 Tz. 7 lit. a MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: a) Spezifizierung und ggf. Abgrenzung der vom Auslagerungsunternehmen zu erbringenden Leistung,	X	X	X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
B.2 - Festlegung der Standorte für die Erbringung von IKT-Dienstleistungen	Der Vertrag muss die Regionen oder Länder angeben, in denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen erbracht werden sowie die Orte, an denen Daten verarbeitet oder gespeichert werden.	Art. 30 Abs. 2 lit. b DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: b) die Standorte — das heißt die Regionen oder Länder —, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen bereitzustellen sind und an denen Daten verarbeitet werden sollen [...] AT 9 Tz. 7 lit. d MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: d) Standorte (d.h. Regionen oder Länder), in denen die Durchführung der Dienstleistung erfolgt und / oder maßgebliche Daten gespeichert und verarbeitet werden, […]	X	X	X	X
B.3 - Festlegung des Ortes der Datenverarbeitung und -speicherung	Der Vertrag muss sicherstellen, dass der Ort der Datenverarbeitung und Datenspeicherung, sowohl für den IKT-Drittdienstleister als auch für Unterauftragnehmer, klar festgelegt wird (z. B. Angabe der Stadt oder, wenn notwendig, die genaue Anschrift)	Art. 30 Abs. 2 lit. b DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: b) die Standorte — das heißt die Regionen oder Länder [...]einschließlich des Speicherorts [...] AT 9 Tz. 7 lit. d MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: d) [...]. Zusätzlich zu Tz. 7 d) muss der Ort der Leistungserbringung (z. B. Stadt oder, sofern notwendig, genaue Anschrift) dem Institut jederzeit bekannt sein. Art. 4 Abs. 1 lit. 3 RTS Subcon: […] für eine Unterauftragsvergabe infrage kommen und unter welchen Bedingungen. In diesem Vertrag wird festgelegt, e) an welchem Ort die Daten vom Unterauftragnehmer gegebenenfalls verarbeitet oder gespeichert werden;	X	X	X	X
B.4 - Benachrichtigung bei Änderungen der Standorte	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister das Finanzunternehmen vorab benachrichtigt, wenn eine Änderung des Standorts der IKT-Dienstleistungen oder der Datenverarbeitung beabsichtigt ist. Dies gilt sowohl für den IKT-Drittdienstleister als auch für Auslagerungsunternehmen bei wesentlichen Auslagerungen.	Art. 30 Abs. 2 lit. b DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: b) [...] die Auflage für den IKT-Drittdienstleister, das Finanzunternehmen vorab zu benachrichtigen, wenn er eine Änderung dieser Standorte beabsichtigt; AT 9 Tz. 7 lit. d MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: d) [...] die Regelung, dass das Institut benachrichtigt wird, wenn das Auslagerungsunternehmen den Standort wechselt,	X	X	X	X
B.5 - Beschreibung der Dienstleistungsgüte und regelmäßige Aktualisierungen	Der Vertrag muss eine angemessene Beschreibung der vereinbarten Dienstleistungsgüte enthalten, einschließlich von Festlegungen zu deren regelmäßiger Aktualisierung und Überarbeitung.	Art. 30 Abs. 2 lit. e DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: e) Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen; AT 9 Tz. 7 lit. e MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: e) vereinbarte Dienstleistungsgüte mit eindeutig festgelegten Leistungsziele	X	X	X	X
B.6 - Vollständige Beschreibung der Dienstleistungsgüte inklusive präziser Leistungsziele	Der Vertrag muss eine umfassende und vollständige Beschreibung der Dienstleistungsgüte für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, enthalten. Dies schließt präzise quantitative und qualitative Leistungsziele sowie Regelungen für Aktualisierungen und Überarbeitungen der Dienstleistungsgüte ein.	AT 9 Tz. 7 lit. e MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: e) vereinbarte Dienstleistungsgüte mit eindeutig festgelegten Leistungsziele Art. 30 Abs. 3 lit. a DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: a) vollständige Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen, mit präzisen quantitativen und qualitativen Leistungszielen innerhalb der vereinbarten Dienstleistungsgüte, um dem Finanzunternehmen eine wirksame Überwachung von IKT-Dienstleistungen und das unverzügliche Ergreifen angemessener Korrekturmaßnahmen zu ermöglichen, wenn eine vereinbarte Dienstleistungsgüte nicht erreicht wird;		X	X	X
B.7 - Festlegung von Leistungsindikatoren und Maßnahmen zur Überwachung der Leistungsfähigkeit	Der Vertrag muss Maßnahmen und Schlüsselindikatoren festlegen, anhand derer die Leistungsfähigkeit des IKT-Drittdienstleisters kontinuierlich überwacht wird.	Art. 9 Abs. 1 RTS TPPol: In der Leitlinie ist vorzusehen, dass in den vertraglichen Vereinbarungen die Maßnahmen und Schlüsselindikatoren festgelegt werden, anhand deren die Leistungsfähigkeit der IKT-Drittdienstleister kontinuierlich überwacht wird […]			X	X
B.8 - Festlegung von Konformitätsindikatoren und Maßnahmen zur Überwachung der Konformität	Der Vertrag muss Maßnahmen und Schlüsselindikatoren festlegen, anhand derer die Einhaltung von Anforderungen in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Daten sowie die Einhaltung von Strategien und Verfahren überwacht werden können (z.B. Kontrollindikatoren, Audits, Selbstzertifizierungen und	Art. 9 Abs. 1 RTS TPPol: In der Leitlinie ist vorzusehen, dass in den vertraglichen Vereinbarungen die Maßnahmen und Schlüsselindikatoren festgelegt werden, anhand deren die Leistungsfähigkeit der IKT-Drittdienstleister kontinuierlich überwacht wird, einschließlich Maßnahmen, die dazu dienen, die Einhaltung der Anforderungen für die			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
	unabhängiger Überprüfungen)	Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Daten und Informationen und die Einhaltung der einschlägigen Strategien und Verfahren des Finanzunternehmens durch die IKT-Drittdienstleister zu überwachen. [...] Art. 9 Abs. 2 lit. b RTS TPPol: […] Die Leitlinie muss insbesondere gewährleisten, dass b) die Leistungsfähigkeit von IKT-Drittdienstleistern anhand wesentlicher Leistungsindikatoren, wesentlicher Kontrollindikatoren, Audits, Selbstzertifizierungen und unabhängiger Überprüfungen im Einklang mit dem IKT- Risikomanagementrahmen des Finanzunternehmens bewertet wird;				
B.9 - Festlegung von Maßnahmen bei Nichteinhaltung der Dienstleistungs-vereinbarungen	Der Vertrag muss Maßnahmen festlegen, die Anwendung finden, wenn die Dienstleistungsvereinbarungen nicht eingehalten werden. Gegebenenfalls müssen auch Vertragsstrafen berücksichtigt werden.	Art. 9 Abs. 1 RTS TPPol: […] Darüber hinaus sind in der Leitlinie Maßnahmen zu spezifizieren, die Anwendung finden, wenn Dienstleistungsvereinbarungen nicht eingehalten werden, und gegebenenfalls Vertragsstrafen umfassen.			X	X
C: Bestimmungen zum Management von Unterauftragnehmern						
C.1 - Regelungen zur Unterauftragsvergabe und Weiterverlagerung	Der Vertrag muss klare Regelungen enthalten, ob und unter welchen Bedingungen der IKT-Drittdienstleister Unteraufträge vergeben oder IKT-Dienstleistungen weiterverlagern darf.	Art. 30 Abs. 2 lit. a DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: a) [...] ob die Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, zulässig ist, und — wenn dies der Fall ist — welche Bedingungen für diese Unterauftragsvergabe gelten; AT 9 Tz. 7 lit. m MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: m) Regelungen über die Möglichkeit und über die Modalitäten einer Weiterverlagerung [...] Art. 4 Abs. 1 RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, welche IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, für eine Unterauftragsvergabe infrage kommen und unter welchen Bedingungen. In diesem Vertrag wird festgelegt,		X	X	X
C.2 - Nachbildung relevanter Vertragsinhalte bei Unteraufträgen	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister bei Unterauftragsvergaben die relevanten Vertragsinhalte nachbildet (z.B. Meldepflichten von IKT-Vorfällen), sodass das Finanzunternehmen weiterhin seine Verpflichtungen aus DORA und anderen geltenden Rechtsvorschriften erfüllen kann.	Art. 3 Abs. 1 lit. c RTS Subcon: der IKT-Drittdienstleister stellt sicher, dass die vertraglichen Vereinbarungen mit den Unterauftragnehmern […] seine eigenen Verpflichtungen aus der Verordnung (EU) 2022/2554 und den geltenden Rechtsvorschriften der Union und der Mitgliedstaaten zu erfüllen; AT 9 Tz. 7 lit. m MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: m) Regelungen [...] die sicherstellen, dass das Institut die bankaufsichtsrechtlichen Anforderungen weiterhin einhält, Art. 4 Abs. 1 lit. i RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, [...] dass die vertragliche Vereinbarung zwischen dem IKT-Drittdienstleister und seinen Unterauftragnehmern die IKT-Sicherheitsstandards und alle zusätzlichen Sicherheitsanforderungen nach Artikel 30 Absatz 3 Buchstabe c der Verordnung (EU) 2022/2554 vorschreibt; Art. 30 Abs. 3 lit. c DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen und über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit seinem Rechtsrahmen bieten;		X	X	X
C.3 - Anforderungen an das Management des IKT-Drittparteienrisikos	Der Vertrag muss den IKT-Drittdienstleister verpflichten, ein ordnungsgemäßes Management des Drittparteienrisikos zu betreiben, insbesondere in Bezug auf Unterauftragnehmer, die kritische oder wichtige IKT-Dienstleistungen für das Finanzunternehmen erbringen.	Art. 8 Abs. 1 RTS TPPol: […] Die Leitlinie umfasst auch Elemente mit Blick auf die in Artikel 1 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Anforderungen sowie gegebenenfalls andere einschlägige Rechtsvorschriften der Union und der Mitgliedstaaten. Art. 1 Abs. 1 lit. a (vi) DORA: […] Maßnahmen für das solide Management des IKT-			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
		Drittparteienrisikos;				
C.4 - Überwachungs- und Berichtspflichten des IKT-Dienstleisters	Der Vertrag muss festlegen, welche Überwachungs- und Berichtspflichten der IKT-Drittdienstleister gegenüber dem Finanzunternehmen in Bezug auf kwF-relevante Unterauftragnehmer hat	Art. 4 Abs. 1 lit. c RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt,[...] c) welche Überwachungs- und Berichtspflichten der IKT-Drittdienstleister gegenüber dem Finanzunternehmen in Bezug auf Unterauftragnehmer hat, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen;			X	X
C.15 - Überwachungs- und Berichterstattungspflichten der Unterauftragnehmer	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister verpflichtet ist, in seinen Verträgen mit Unterauftragnehmern die Überwachungs- und Berichtspflichten zu vereinbaren. Sofern mit dem Finanzunternehmen vereinbart, muss der IKT-Dienstleister auch verpflichtet werden, direkte Berichtspflichten der Unterauftragnehmer an das Finanzunternehmen in seine Verträge mit den Unterauftragnehmern aufzunehmen.	Art. 4 Abs. 1 lit. f RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, [...] , f) dass der IKT-Drittdienstleister in seinem Vertrag mit seinen Unterauftragnehmern die Überwachungs- und Berichterstattungspflichten dieses Unterauftragnehmers gegenüber dem IKT-Drittdienstleister und, sofern vereinbart, gegenüber dem Finanzunternehmen festzulegen hat;			X	X
C.6 - Zugangs-, Inspektions- und Auditrechte bei Unterauftragnehmern	Der Vertrag muss sicherstellen, dass der IKT-Dienstleister verpflichtet wird, die Rechte auf fortlaufende Überwachung in seinen Verträgen mit Unterauftragnehmern nachzubilden. Dies umfasst: • Uneingeschränkte Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder beauftragter Dritter sowie der zuständigen Behörde, einschließlich des Rechts zur Anfertigung von Kopien einschlägiger Unterlagen vor Ort; • Das Recht auf alternative Bestätigungsniveaus, wenn die Rechte anderer Kunden betroffen sind; • Die Verpflichtung zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits • Die Mitteilung von Einzelheiten zu Umfang, Häufigkeit und dem Verfahren dieser Inspektionen und Audits.	Art. 4 Abs. 1 lit. j RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, welche IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, für eine Unterauftragsvergabe infrage kommen und unter welchen Bedingungen. In diesem Vertrag wird festgelegt, j) dass der Unterauftragnehmer dem Finanzunternehmen und den relevanten zuständigen Behörden und Abwicklungsbehörden dieselben Zugangs-, Inspektions- und Auditrechte wie die in Artikel 30 Absatz 3 Buchstabe e der Verordnung (EU) 2022/2254 genannten gewähren muss; Art. 30 Abs. 3 lit. e DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört: • i) uneingeschränkte Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten und der zuständigen Behörde sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort, wenn ihnen für die Geschäftstätigkeit des IKT-Drittdienstleisters entscheidende Bedeutung zukommt, wobei die tatsächliche Ausübung dieser Rechte nicht durch andere vertragliche Vereinbarungen oder Umsetzungsrichtlinien behindert oder eingeschränkt wird; • ii) das Recht, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind; • iii) die Verpflichtung des IKT-Drittdienstleisters zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, dem Finanzunternehmen oder einem beauftragten Dritten durchgeführt werden; und • iv) die Verpflichtung, Einzelheiten zu Umfang und Häufigkeit dieser Inspektionen sowie dem dabei zu befolgenden Verfahren mitzuteilen;			X	X
C.7 - IKT-Sicherheitsstandards und Notfallpläne bei Unterauftragnehmern	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister verpflichtet wird, die Festlegungen zu IKT-Sicherheitsstandards, einschließlich der Bereitstellung von Maßnahmen, Tools, Richtlinien für IKT-Sicherheit sowie der Implementierung und Testung von Notfallplänen, in seinen Verträgen mit den Unterauftragnehmern nachzubilden, um ein angemessenes Maß an Sicherheit für die Erbringung von IKT-Dienstleistungen durch die Unterauftragnehmer zu gewährleisten.	Art. 4 Abs. 1 lit. i RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, [...]dass die vertragliche Vereinbarung zwischen dem IKT-Drittdienstleister und seinen Unterauftragnehmern die IKT-Sicherheitsstandards und alle zusätzlichen Sicherheitsanforderungen nach Artikel 30 Absatz 3 Buchstabe c der Verordnung (EU) 2022/2554 vorschreibt; Art. 4 Abs. 1 lit. h RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, [...] dass die vertragliche Vereinbarung zwischen dem IKT-Drittdienstleister und seinen Unterauftragnehmern die in Artikel 30 Absatz 3 Buchstabe c der Verordnung (EU)			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
		2022/2554 genannten Anforderungen an Geschäftsfortführungspläne enthält und die von den IKT-Unterauftragnehmern in Bezug auf diese Pläne zu erfüllende Dienstleistungsgüte vorschreibt; Art. 30 Abs. 3 lit. c DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen und über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit seinem Rechtsrahmen bieten;				
C.8 - Überwachung von Unterauftragnehmern durch den IKT-Drittdienstleister	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister alle an Unterauftragnehmer vergebenen IKT-Dienstleistungen die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, überwacht.	Art. 4 Abs. 1 lit. b RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, welche IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, für eine Unterauftragsvergabe infrage kommen und unter welchen Bedingungen. In diesem Vertrag wird festgelegt, b) dass der IKT-Drittdienstleister verpflichtet ist, alle an Unterauftragnehmer vergebenen IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, zu überwachen, um sicherzustellen, dass seine vertraglichen Verpflichtungen gegenüber dem Finanzunternehmen jederzeit erfüllt werden;			X	X
C.9 - Sicherstellung der Kontinuität der IKT-Dienstleistungen entlang der Unterauftragnehmer-kette	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister die Kontinuität der IKT-Dienstleistungen entlang der gesamten Kette von kwF-relevanten Unterauftragnehmern sicherstellen muss, insbesondere wenn ein IKT-Unterauftragnehmer seinen vertraglichen Verpflichtungen nicht nachkommt.	Art. 4 Abs. 1 lit. g RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, welche IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, für eine Unterauftragsvergabe infrage kommen und unter welchen Bedingungen. In diesem Vertrag wird festgelegt, g) dass der IKT-Drittdienstleister die Kontinuität der IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, entlang der gesamten Kette von Unterauftragnehmern sicherstellen muss, wenn ein IKT-Unterauftragnehmer seinen vertraglichen Verpflichtungen nicht nachkommt;			X	X
C.10 - Risikobewertung von Unterauftragnehmern	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister alle Risiken bewertet, die mit dem Standort der Unterauftragnehmer und ihres Mutterunternehmens sowie dem Standort, von dem aus die IKT-Dienstleistung erbracht wird, verbunden sind.	Art. 4 Abs. 1 lit. d RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, welche IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, für eine Unterauftragsvergabe infrage kommen und unter welchen Bedingungen. In diesem Vertrag wird festgelegt, d) dass der IKT-Drittdienstleister alle Risiken zu bewerten hat, die mit dem Standort der derzeitigen oder potenziellen Unterauftragnehmer, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon erbringen, und ihres Mutterunternehmens sowie mit dem Standort, von dem aus die betreffende IKT-Dienstleistung erbracht wird, verbunden sind;			X	X
C.11 - Anzeigepflicht von wesentlichen Änderungen der Unterauftragsvergabe	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister das Finanzunternehmen rechtzeitig über alle beabsichtigten wesentlichen Änderungen seiner Unterauftragsvereinbarungen informiert und jede wesentliche Änderung der Unterauftragsvereinbarungen meldet.	Art. 4 Abs. 1 lit. k RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, [...] k) dass der IKT-Drittdienstleister dem Finanzunternehmen jede wesentliche Änderung der Unterauftragsvereinbarungen zu melden hat; Art. 5 Abs. 1 RTS Subcon: Die vertragliche Vereinbarung sieht vor, dass der IKT-Drittdienstleister das Finanzunternehmen rechtzeitig über alle beabsichtigten wesentlichen Änderungen seiner Unterauftragsvereinbarungen informiert[...]			X	X
C.12 - Umsetzung von Änderungen der Unterauftrags-vereinbarungen	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister wesentliche Änderungen seiner Unterauftragsvereinbarungen erst umsetzt, wenn das Finanzunternehmen die Änderungen bis zum Ablauf der Mitteilungsfrist entweder genehmigt oder sie nicht abgelehnt hat.	Art. 5 Abs. 3 RTS Subcon: Der IKT-Drittdienstleister setzt die wesentlichen Änderungen seiner Unterauftragsvereinbarungen erst dann um, wenn das Finanzunternehmen die Änderungen bis zum Ablauf der Mitteilungsfrist entweder genehmigt oder sie nicht abgelehnt hat.			X	X
C.13 - Mitteilungsfrist für Änderungen der Unterauftrags-vereinbarungen	Der Vertrag muss eine angemessene Mitteilungsfrist festlegen, innerhalb derer das Finanzunternehmen den Änderungen der Unterauftragsvereinbarungen zustimmen oder sie ablehnen kann.	Art. 5 Abs. 2 RTS Subcon: Die vertragliche Vereinbarung muss eine angemessene Mitteilungsfrist enthalten, in der das Finanzunternehmen den Änderungen zustimmen oder sie ablehnen kann. Art. 5 Abs. 4 RTS Subcon: Ist das Finanzunternehmen der Auffassung, dass die in Absatz 1 genannten wesentlichen Änderungen die Risikotoleranz des Finanzunternehmens überschreiten, so muss es vor Ablauf der Mitteilungsfrist a) den			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
		IKT-Drittdienstleister davon in Kenntnis setzen; b) die Änderungen ablehnen und vor deren Umsetzung Anpassungen verlangen.				
C.14 - Ablehnung und Anpassung von Änderungen der Unterauftrags-vereinbarungen	Der Vertrag muss sicherstellen, dass das Finanzunternehmen die Änderungen an den Unterauftragsvereinbarungen ablehnen und Anpassungen vor deren Umsetzung verlangen kann.	Art. 29 Abs. 2 DORA: Ist in der vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen die Möglichkeit vorgesehen, dass ein IKT-Drittdienstleister IKT-Dienstleistungen zur Unterstützung einer kritischen oder wichtigen Funktion per Unterauftrag an andere IKT-Drittdienstleister vergibt, wägen Finanzunternehmen die Vorteile und Risiken ab, die im Zusammenhang mit einer solchen Unterauftragsvergabe entstehen können, insbesondere sofern der IKT-Unterauftragnehmer in einem Drittland niedergelassen ist. Art. 5 Abs. 1 RTS Subcon: Die vertragliche Vereinbarung sieht vor, dass der IKT-Drittdienstleister das Finanzunternehmen rechtzeitig über alle beabsichtigten wesentlichen Änderungen seiner Unterauftragsvereinbarungen informiert, damit das Finanzunternehmen Folgendes bewerten kann: a) die Auswirkung auf die Risiken, denen er ausgesetzt ist oder ausgesetzt sein könnte; b) ob solche wesentlichen Änderungen die Fähigkeit des IKT-Drittdienstleisters beeinträchtigen könnten, seinen vertraglichen Verpflichtungen gegenüber dem Finanzunternehmen nachzukommen. Art. 5 Abs. 4 RTS Subcon: Ist das Finanzunternehmen der Auffassung, dass die in Absatz 1 genannten wesentlichen Änderungen die Risikotoleranz des Finanzunternehmens überschreiten, so muss es vor Ablauf der Mitteilungsfrist a) den IKT-Drittdienstleister davon in Kenntnis setzen; b) die Änderungen ablehnen und vor deren Umsetzung Anpassungen verlangen.			X	X
D: Bestimmungen zum IKT-Risikomanagementrahmen						
D.1 - Festlegungen zu Datenschutz und Schutz personenbezogener Daten	Der Vertrag muss Bestimmungen zum Schutz personenbezogener Daten enthalten, einschließlich der Einhaltung von Datenschutzvorgaben.	Art. 30 Abs. 2 lit. c DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: c) Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten; AT 9 Tz. 7 lit. k MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: k) Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen beachtet werden,	X	X	X	X
D.2 - Festlegungen zu Informationssicherheit und Schutz von Informationen	Der Vertrag muss Regelungen zur Informationssicherheit und zum Schutz wesentlicher Daten beinhalten. Dies umfasst spezifische Bestimmungen zur Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten.	Art. 30 Abs. 2 lit. c DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: c) Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten; AT 9 Tz. 7 lit. k MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: k) Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen beachtet werden, Sonstige Sicherheitsanforderungen: Regelungen zu sonstigen Sicherheitsanforderungen sollten für alle, also auch nicht wesentliche Auslagerungen, vertraglich vereinbart werden. Zu den sonstigen Sicherheitsanforderungen zählen vor allem Zugangsbestimmungen zu Räumen und Gebäuden (z. B. bei Rechenzentren) sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen. Die Einhaltung dieser Anforderungen ist fortlaufend zu überwachen. Institute sollten einen risikobasierten Ansatz betreffend den Standort der Datenspeicherung und Datenverarbeitung sowie hinsichtlich der Informationssicherheit wählen. [...]	X	X	X	X
D.3 – Teilnahmebedingungen an Schulungsprogrammen	Der Vertrag muss Bedingungen für die Teilnahme des IKT-Dienstleisters an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operativen Resilienz festlege	Art. 30 Abs. 2 lit. i DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: i) Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz gemäß Artikel 13 Absatz 6.	X		X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
D.4 - Anforderungen an die Daten- und Systemsicherheit	Der Vertrag muss die Bewertung der Kritikalität/ Klassifizierung der IKT-Assets aus Sicht des Finanzunternehmens enthalten sowie die damit verbundenen Anforderungen an die digitale operationale Resilienz der IKT-Dienstleistungen, die vom Dienstleister bereitgestellt werden.	Art. 11 Abs 2 lit. k RTS RMF: Das in Absatz 1 genannte Verfahren für die Daten- und Systemsicherheit umfasst alle folgenden Elemente im Zusammenhang mit der Daten- und IKT-Systemsicherheit im Einklang mit der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung: k) für IKT-Assets oder -Dienstleistungen, die von einem IKT- Drittdienstleister betrieben werden, die Ermittlung und Umsetzung von Anforderungen an die Aufrechterhaltung der digitalen operationalen Resilienz im Einklang mit den Ergebnissen der Datenklassifizierung und der IKT-Risikobewertung. Für die Zwecke von Buchstabe k berücksichtigen Finanzunternehmen Folgendes: a) die Implementierung der vom Anbieter empfohlenen Einstellungen für Komponenten, die vom Finanzunternehmen betrieben werden; b) eine klare Aufteilung der die Informationssicherheit betreffenden Aufgaben und Verantwortlichkeiten zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister im Einklang mit dem in Artikel 28 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Grundsatz der vollen Verantwortlichkeit des Finanzunternehmens für seinen IKT-Drittdienstleister und für Finanzunternehmen nach Artikel 28 Absatz 2 der genannten Verordnung sowie im Einklang mit der Richtlinie des Finanzunternehmens für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen;	X		X	X
D.5 - Anforderungen an die Netzwerksicherheit	Der Vertrag muss Bestimmungen zu technischen und organisatorischen Maßnahmen für die Netzwerksicherheit beim IKT-Dienstleister enthalten, um Risiken für die Daten des Finanzunternehmens zu minimieren, die sich aus der Verarbeitung und Speicherung dieser Daten in der Infrastruktur des IKT-Dienstleisters ergeben. Dabei sind führende Praktiken und Normen zu berücksichtigen.	Art. 11 Abs 2 lit. k (d) RTS RMF: Das in Absatz 1 genannte Verfahren für die Daten- und Systemsicherheit umfasst alle folgenden Elemente im Zusammenhang mit der Daten- und IKT-Systemsicherheit im Einklang mit der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung: k) für IKT-Assets oder -Dienstleistungen, die von einem IKT- Drittdienstleister betrieben werden, die Ermittlung und Umsetzung von Anforderungen an die Aufrechterhaltung der digitalen operationalen Resilienz im Einklang mit den Ergebnissen der Datenklassifizierung und der IKT-Risikobewertung. Für die Zwecke von Buchstabe k berücksichtigen Finanzunternehmen Folgendes: d) technische und organisatorische Maßnahmen zur Minimierung der Risiken im Zusammenhang mit der Infrastruktur, die der IKT-Drittdienstleister für seine IKT-Dienstleistungen nutzt, unter Berücksichtigung führender Praktiken und Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012.	X		X	X
D.6 - Spezifikation Sicherheitsmaßnahmen für Network Services Agreements:	Verträge, die Netzwerkdienstleistungen (z.B. Netzwerkmanagement) betreffen, müssen Sicherheitsmaßnahmen, Dienstleistungsgüte und Anforderungen an das Management dieser Dienste festlegen. Zusätzlich muss der Vertrag klären, ob die Netzwerkdienstleistungen von einem gruppeninternen IKT-Dienstleister oder einem IKT-Drittdienstleister erbracht werden.	Art. 13 lit. m RTS RMF: Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der Schutzvorkehrungen, die die Sicherheit der Netzwerke gegen Eindringen und Missbrauch von Daten gewährleisten, Richtlinien, Verfahren, Protokolle und Tools für das Management der Netzwerksicherheit, in denen alle folgenden Aspekte behandelt werden: m) für Vereinbarungen über Netzwerkdienstleistungen: i) die Ermittlung und Spezifikation von IKT- und Informationssicherheitsmaßnahmen, der Dienstleistungsgüte und von Managementanforderungen für alle Netzwerkdienste; ii) die Feststellung, ob diese Dienstleistungen von einem gruppeninternen IKT-Dienstleister oder von IKT- Drittdienstleistern erbracht werden.	X		X	X
D.7 - Anforderungen an IKT-Sicherheitsmaßnahmen, Tools und Richtlinien	Der Vertrag muss vorschreiben, dass der IKT-Drittdienstleister über die erforderlichen Maßnahmen, Tools und Richtlinien für die IKT-Sicherheit verfügt und diese kontinuierlich aufrechterhält,, um die Sicherheit der erbrachten IKT-Dienstleistungen im Einklang mit dem Rechtsrahmen des Finanzunternehmens zu gewährleisten.	Art. 30 Abs. 3 lit. c DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: c) Anforderungen an den IKT-Drittdienstleister […] über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit seinem Rechtsrahmen bieten;			X	X
D.8 - Anforderungen an das IKT-Risikomanagement	Der Vertrag muss Anforderungen an das IKT-Risikomanagement des Dienstleisters festlegen.	Art. 8 Abs. 1 RTS TPPol: In der Leitlinie wird festgelegt, dass die einschlägige vertragliche Vereinbarung schriftlich abzufassen ist und alle in Artikel 30 Absätze 2 und 3 der Verordnung (EU) 2022/2554 genannten Elemente enthalten muss. Die Leitlinie umfasst auch Elemente mit Blick auf die in Artikel 1 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Anforderungen sowie gegebenenfalls andere einschlägige Rechtsvorschriften der Union und der Mitgliedstaaten.			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
		Art. 1 Abs. 1 lit. a (i) DORA: […] Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT);				
D.9 - Anforderungen an die Bereitstellung von Informationen zu Cyberbedrohungen und Schwachstellen	Der Vertrag muss Anforderungen an die Meldung von Cyberbedrohungen und Schwachstellen beinhalten.	Art. 8 Abs. 1 RTS TPPol: In der Leitlinie wird festgelegt, dass die einschlägige vertragliche Vereinbarung schriftlich abzufassen ist und alle in Artikel 30 Absätze 2 und 3 der Verordnung (EU) 2022/2554 genannten Elemente enthalten muss. Die Leitlinie umfasst auch Elemente mit Blick auf die in Artikel 1 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Anforderungen sowie gegebenenfalls andere einschlägige Rechtsvorschriften der Union und der Mitgliedstaaten. Art. 1 Abs. 1 lit. a (v) DORA: […] Austausch von Informationen und Erkenntnissen in Bezug auf Cyberbedrohungen und Schwachstellen;			X	X
D.10 - Anforderungen an Tests der digitalen operationalen Resilienz	Der Vertrag muss Anforderungen an den IKT-Dienstleister zur durchführung regelmäßiger Tests der digitalen operationalen Resilienz enthalten.	Art. 8 Abs. 1 RTS TPPol: In der Leitlinie wird festgelegt, dass die einschlägige vertragliche Vereinbarung schriftlich abzufassen ist und alle in Artikel 30 Absätze 2 und 3 der Verordnung (EU) 2022/2554 genannten Elemente enthalten muss. Die Leitlinie umfasst auch Elemente mit Blick auf die in Artikel 1 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Anforderungen sowie gegebenenfalls andere einschlägige Rechtsvorschriften der Union und der Mitgliedstaaten. Art. 1 Abs. 1 lit. a (iv) DORA: […] Tests der digitalen operationalen Resilienz;			X	X
D.11 - Festlegungen zur Durchführung von IKT-Tests	Der Vertrag muss Regelungen zur Durchführung von IKT-Tests, einschließlich potenzieller TLPTs, enthalten. Zu den möglichen IKT-Tests gemäß Art. 25 (1) DORA gehören weiterhin Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.	Art. 8 Abs. 2 lit. b RTS TPPol: IIn der Leitlinie ist festzulegen, dass die einschlägigen vertraglichen Vereinbarungen das Recht des Finanzunternehmens auf Zugang zu Informationen, auf die Durchführung von Inspektionen und Audits sowie auf die Durchführung von IKT-Tests vorsehen müssen. In der Leitlinie ist vorzusehen, dass das Finanzunternehmen zu diesen Zwecken — unbeschadet seiner letztlichen Verantwortung — auf folgende Methoden zurückgreifen muss: [...] b) gegebenenfalls Sammelaudits und gepoolte IKT-Tests, einschließlich bedrohungsorientierter Penetrationstests, die gemeinsam mit anderen als Auftraggeber auftretenden Finanzunternehmen oder Firmen, die IKT-Dienstleistungen desselben IKT-Drittdienstleisters nutzen, organisiert und von diesen Finanzunternehmen oder Firmen oder einem von ihnen beauftragten Dritten durchgeführt werden; Art. 25 Abs. 1 DORA: Das in Artikel 24 genannte Programm für die Tests der digitalen operationalen Resilienz beinhaltet im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien die Durchführung angemessener 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 und Penetrationstests.			X	X
D.12 - Verpflichtung zur Teilnahme an TLPP	Der Vertrag muss den IKT-Drittdienstleister verpflichten, sich uneingeschränkt an den TLPTs des Finanzunternehmens zu beteiligen und aktiv daran mitzuwirken.	Art. 30 Abs. 3 lit. d DORA: die Verpflichtung des IKT-Drittdienstleisters, sich an den in den Artikeln 26 und 27 genannten TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken;			X	X
D.13 - Optionale Vereinbarung über gebündelte TLPTs	Der Vertrag kann es dem IKT-Drittdienstleister ermöglichen, eine vertragliche Vereinbarung mit einem externen Tester für einen gebündelten TLPT unter der Leitung des Finanzunternehmens zu treffen, um nachteilige Auswirkungen auf Qualität, Sicherheit oder Vertraulichkeit der Dienstleistungen oder Daten zu begrenzen.	Art. 26 Abs. 44 DORA: Wenn vernünftigerweise davon auszugehen ist, dass sich die Einbindung eines IKT-Drittdienstleisters in einen TLPT gemäß Absatz 3 nachteilig auf die Qualität oder die Sicherheit von Dienstleistungen des IKT-Drittdienstleisters an Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, oder auf die Vertraulichkeit in Bezug auf die mit diesen Dienstleistungen verbundenen Daten auswirkt, können das Finanzunternehmen und der IKT-Drittdienstleister unbeschadet Absatz 2 Unterabsätze 1 und 2 schriftlich vereinbaren, dass der IKT- Drittdienstleister unmittelbar vertragliche Vereinbarungen mit einem externen Tester schließt, um unter der Leitung eines benannten Finanzunternehmens einen gebündelten TLPT durchzuführen, an dem mehrere Finanzunternehmen beteiligt sind (gebündelter Test), für die der IKT-Drittdienstleister IKT-Dienstleistungen erbringt.			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
E: Bestimmungen zum IKT-BCM und Management von IKT-Vorfällen						
E.1 - Unterstützung bei IKT-Vorfällen	Der Vertrag muss den IKT-Drittdienstleister verpflichten, dem Finanzunternehmen bei einem IKT-Vorfall, der mit der bereitgestellten Dienstleistung in Verbindung steht, Unterstützung zu leisten.	Art. 30 Abs. 2 lit. f DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: f) die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten;	X	X	X	X
E.2 - Regelung der Vergütung für Unterstützung bei IKT-Vorfällen	Der Vertrag muss festlegen, dass die Unterstützung des IKT-Drittdienstleisters bei IKT-Vorfällen ohne zusätzliche Kosten oder zu vorab festzulegenden Kosten erfolgt.	Art. 30 Abs. 2 lit. f DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: f) die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten;	X	X	X	X
E.3 - Vorgaben für Wiederherstellungszeit und -punkte	Der Vertrag muss Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte jeder Funktion festlegen, wobei berücksichtigt wird, ob es sich um eine kritische oder wichtige Funktion handelt. Diese Vorgaben müssen sicherstellen, dass die vereinbarte Dienstleistungsgüte auch in Extremszenarien erreicht wird.	Art. 12 Abs. 6 DORA: Bei der Festlegung der Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte jeder Funktion berücksichtigen die Finanzunternehmen, ob es sich um eine kritische oder wichtige Funktion handelt, sowie die potenziellen Gesamtauswirkungen auf die Markteffizienz. Mit diesen Zeitvorgaben ist sichergestellt, dass die vereinbarte Dienstleistungsgüte in Extremszenarien erreicht werden.	(x)	X	X	X
E.4 - Meldung von IKT-Vorfällen durch den IKT-Dienstleister	Der Vertrag muss den IKT-Drittdienstleister verpflichten, das Finanzunternehmen über schwerwiegende IKT-Vorfälle und erhebliche Cyberbedrohungen zu informieren, die die erbrachten IKT-Dienstleistungen betreffen, damit das Finanzunternehmen seine Meldepflichten erfüllen kann.	Art. 8 Abs. 1 RTS TPPol: […] Die Leitlinie umfasst auch Elemente mit Blick auf die in Artikel 1 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Anforderungen sowie gegebenenfalls andere einschlägige Rechtsvorschriften der Union und der Mitgliedstaaten. Art. 1 Abs. 1 lit. a (ii) DORA: […] ii) Meldung schwerwiegender IKT-bezogener Vorfälle und — auf freiwilliger Basis — erheblicher Cyberbedrohungen an die zuständigen Behörden; Art. 9 Abs. 2 lit. d RTS TPPol: […] Die Leitlinie muss insbesondere gewährleisten, dass d) das Finanzunternehmen gegebenenfalls über IKT-bezogene Vorfälle […] Vorfälle im Zusammenhang mit Zahlungen unterrichtet wird; Art. 9 Abs. 2 lit. a RTS TPPol: […] Die Leitlinie muss insbesondere gewährleisten, dass a) die IKT-Drittdienstleister dem Finanzunternehmen angemessene [...] Berichte über Vorfälle			X	X
E.5 - Meldung schwerwiegender zahlungsbezogener Vorfälle	Der Vertrag muss den IKT-Drittdienstleister verpflichten, das Finanzunternehmen über schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle zu informieren, die die erbrachten IKT-Dienstleistungen betreffen, damit das Finanzunternehmen seine Meldepflichten gegenüber den zuständigen Behörden erfüllen kann.	Art. 8 Abs. 1 RTS TPPol: […] Die Leitlinie umfasst auch Elemente mit Blick auf die in Artikel 1 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Anforderungen sowie gegebenenfalls andere einschlägige Rechtsvorschriften der Union und der Mitgliedstaaten. Art. 1 Abs. 1 lit. a (ii): […] Meldung schwerwiegender IKT-bezogener Vorfälle und — auf freiwilliger Basis — erheblicher Cyberbedrohungen an die zuständigen Behörden; Art. 9 Abs. 2 lit. d RTS TPPol: […]. Die Leitlinie muss insbesondere gewährleisten, dass d) das Finanzunternehmen gegebenenfalls über […] operationale oder sicherheitsbezogene Vorfälle im Zusammenhang mit Zahlungen unterrichtet wird; Art. 9 Abs. 2 lit. a RTS TPPol: In der Leitlinie wird festgelegt, wie das Finanzunternehmen bewertet, ob die IKT-Drittdienstleister, die für die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen in Anspruch genommen werden, angemessene Leistungs- und Qualitätsstandards im Einklang mit der vertraglichen Vereinbarung und den Strategien des Finanzunternehmens einhalten. Die Leitlinie muss insbesondere gewährleisten, dass a) die IKT-Drittdienstleister dem Finanzunternehmen angemessene [...] Berichte über Vorfälle Art. 9 Abs. 2 lit. d RTS TPPol: […]. Die Leitlinie muss insbesondere gewährleisten, dass d) das Finanzunternehmen gegebenenfalls über IKT-bezogene Vorfälle und operationale oder sicherheitsbezogene Vorfälle im Zusammenhang mit Zahlungen unterrichtet wird;			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
E.6 - Anforderungen an die Umsetzung und Überprüfung eines Notfallkonzeptes	Der Vertrag muss Anforderungen für die Umsetzung und Überprüfung von Notfallkonzepten festlegen. Hierzu zählen beispielsweise Notfallvorsorgekonzept zum Schutz vor Notfällen, Notfallhandbuch, Wiederherstellungspläne, Geschäftsfortführungspläne sowie Kommunikationspläne.	AT 9 Tz. 7 lit. g MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: g) Anforderungen für die Umsetzung und Überprüfung von Notfallkonzepten,		X		X
E.7 - Implementierung und Test von Notfallplänen durch den IKT-Drittdienstleister	Der Vertrag muss vom IKT-Drittdienstleister verlangen, dass Notfallpläne für kritische oder wichtige Funktionen implementiert und regelmäßig getestet werden. Diese Notfallpläne müssen sicherstellen, dass die erforderlichen Maßnahmen zur Fortführung und Wiederherstellung der Dienste im Notfall ergriffen werden, und es müssen geeignete Tools, Maßnahmen und Richtlinien für die IKT-Sicherheit vorhanden sein.	Art. 30 Abs. 3 lit. c DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: c) Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen und über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit seinem Rechtsrahmen bieten;			X	X
E.8 - Vereinbarungen zur Unterstützung des IKT-Drittdienstleisters beim Testen von IKT-Geschäftsfort-führungsplänen	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister das Finanzunternehmen beim Testen und Überprüfen der IKT-Geschäftsfortführungspläne insbesondere mit Bezug zu kwF unterstützt.	Art. 11 Abs. 4 DORA: Finanzunternehmen erstellen, pflegen und testen regelmäßig angemessene IKT-Geschäftsfortführungspläne, insbesondere in Bezug auf kritische oder wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittdienstleister vergeben werden.			X	X
F: Bestimmungen zu Kündigung und Exit						
F.1 - Regelungen zur Wiederherstellung und Rückgabe von Daten im Exit-Fall	Der Vertrag muss Bestimmungen enthalten, die sicherstellen, dass im Falle einer Insolvenz, Abwicklung oder der Beendigung der vertraglichen Vereinbarungen die Wiederherstellung und Rückgabe der verarbeiteten Daten in einem leicht zugänglichen Format gewährleistet wird.	Art. 30 Abs. 2 lit. d DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: d) Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT- Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format;	X	X	X	X
F.2 - Zugang und Zugriff zu Daten und Räumlichkeiten im Exit-Fall	Der Vertrag muss sicherstellen, dass das Finanzunternehmen, seine Revisoren und die zuständigen Behörden im Falle einer Insolvenz, Abwicklung oder der Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters Zugang zu den Räumlichkeiten des IKT-Dienstleisters und den im Eigentum befindlichen Daten haben	AT 9 Tz. 7 lit. k MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: k) Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen beachtet werden. Sonstige Sicherheitsanforderungen: [...] Es ist sicherzustellen, dass auf die sich im Eigentum des Instituts befindlichen Daten im Fall einer Insolvenz, Abwicklung oder der Einstellung der Geschäftstätigkeit des Auslagerungsunternehmens zugegriffen werden kann. Art. 30 Abs. 2 lit. d DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: d) Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT- Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format;	X	X	X	X
F.3 - Allgemeine Kündigungsrechte und Mindest-kündigungsfristen	Der Vertrag muss Kündigungsrechte und Mindestkündigungsfristen festlegen, die den Anforderungen der zuständigen Behörden und Abwicklungsbehörden entsprechen.	Art. 30 Abs. 2 lit. h DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: h) Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und der Abwicklungsbehörden; AT 9 Tz. 7 lit. l MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: l) Kündigungsrechte und angemessene Kündigungsfristen, Art. 30 Abs. 3 lit. b DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: b) Kündigungsfristen und Berichtspflichten des IKT-Drittdienstleisters gegenüber dem Finanzunternehmen, [...]	X	X	X	X
F.4 - Kündigungsrechte bei Verstößen und Risiken des IKT-Dienstleisters	Der Vertrag muss dem Finanzunternehmen das Recht geben, die Vereinbarung mit dem IKT-Drittdienstleister zu kündigen, wenn: • Ein erheblicher Verstoß gegen Gesetze, Vorschriften oder Vertragsbedingungen vorliegt.	Art. 28 Abs. 7 DORA: Finanzunternehmen stellen sicher, dass vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen gekündigt werden können, wenn einer der folgenden Umstände vorliegt: • a) ein erheblicher Verstoß des IKT-Drittdienstleisters gegen geltende Gesetze,	X	X	X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
	• Überwachte Umstände die Erbringung der vereinbarten Funktionen beeinträchtigen könnten. • Schwächen im IKT-Risikomanagement des Dienstleisters festgestellt werden. • Die zuständige Behörde das Finanzunternehmen nicht mehr wirksam beaufsichtigen kann.	sonstige Vorschriften oder Vertragsbedingungen; • b) Umstände, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT- Drittdienstleisters auswirken; • c) nachweisliche Schwächen des IKT-Drittdienstleisters in Bezug auf sein allgemeines IKT-Risikomanagement und insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt; • d) die zuständige Behörde kann das Finanzunternehmen infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen.				
F.5 - Unterstützung bei der Übertragung oder Reintegration der ausgelagerten Aktivitäten	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister das Finanzunternehmen bei der Übertragung der ausgelagerten Aktivitäten oder deren Reintegration ins Unternehmen unterstützt, wenn die vertragliche Vereinbarung gekündigt wird.	AT 9 Tz. 7 lit. l MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: l) Kündigungsrechte und angemessene Kündigungsfristen, Kündigungsrechte Die Auslagerungsvereinbarung sollte das Auslagerungsunternehmen für den Fall einer Kündigung verpflichten, das Institut bei der Übertragung der ausgelagerten Aktivität bzw. des ausgelagerten Prozesses an ein anderes Auslagerungsunternehmen oder ihre bzw. seine Reintegration in das Institut zu unterstützen.		X		X
F.6 - Kündigungsrechte bei Verstößen und Risiken in Zusammenhang mit Unterauftragnehmern	Der Vertrag muss sicherstellen, dass das Finanzunternehmen das Recht hat, den Vertrag mit dem IKT-Drittdienstleister zu kündigen, wenn eines der folgenden Szenarien eintritt: • a) Das Finanzunternehmen hat wesentliche Änderungen der Unterauftragsvereinbarungen abgelehnt und Anpassungen verlangt, doch der IKT-Drittdienstleister hat diese Änderungen dennoch umgesetzt. • b) Der IKT-Drittdienstleister hat wesentliche Änderungen an den Unterauftragsvereinbarungen vorgenommen, ohne die Genehmigung des Finanzunternehmens und vor Ablauf der Mitteilungsfrist. • c) Der IKT-Drittdienstleister hat eine IKT-Dienstleistung, die kritische oder wichtige Funktionen unterstützt, ohne ausdrückliche Genehmigung des Finanzunternehmens als Unterauftrag vergeben.	Art. 4 Abs. 1 lit. l RTS Subcon In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, welche IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, für eine Unterauftragsvergabe infrage kommen und unter welchen Bedingungen. In diesem Vertrag wird festgelegt, l) dass das Finanzunternehmen das Recht hat, den Vertrag mit dem IKT-Drittdienstleister zu kündigen, wenn die in Artikel 6 der vorliegenden Verordnung oder die in Artikel 28 Absatz 7 der Verordnung (EU) 2022/2554 beschriebenen Bedingungen erfüllt sind. Art. 6 RTS Subcon: Das Finanzunternehmen hat das Recht, in der vertraglichen Vereinbarung mit dem IKT-Drittdienstleister vorzusehen, dass die vertragliche Vereinbarung in jedem der folgenden Fälle beendet wird: a) Das Finanzunternehmen hat wesentliche Änderungen der Unterauftragsvereinbarungen zur Unterstützung kritischer oder wichtiger Funktionen abgelehnt und um Anpassungen dieser Änderungen gebeten, doch der IKT-Drittdienstleister hat diese wesentlichen Änderungen dennoch umgesetzt; b) der IKT-Drittdienstleister hat vor Ablauf der Mitteilungsfrist ohne Genehmigung des Finanzunternehmens wesentliche Änderungen an den Unterauftragsvereinbarungen zur Unterstützung kritischer oder wichtiger Funktionen oder wesentlicher Teile davon vorgenommen; c) der IKT-Drittdienstleister hat eine IKT-Dienstleistung, die eine kritische oder wichtige Funktion oder einen wesentlichen Teil davon unterstützt, als Unterauftrag vergeben, obwohl eine derartige Unterauftragsvergabe im Vertrag zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister nicht ausdrücklich genehmigt wurde.			X	X
F.7 - Vereinbarung einer Ausstiegsstrategie	Der Vertrag muss eine Ausstiegsstrategie vereinbaren, die sicherstellt, dass das Finanzunternehmen im Falle eines Ausstiegs aus dem Vertrag keine Störungen in der Geschäftstätigkeit erleidet und die Kontinuität sowie Qualität der erbrachten IKT-Dienstleistungen gewährleistet bleibt. Diese Strategie muss einen angemessenen Übergangszeitraum umfassen, in dem der IKT-Drittdienstleister weiterhin die IKT-Dienstleistungen bereitstellt.	Art. 30 Abs. 3 lit. f (i) DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: f) Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums, i) in dem der IKT-Drittdienstleister weiterhin die entsprechenden Funktionen oder IKT-Dienstleistungen bereitstellt, um das Risiko von Störungen im Finanzunternehmen zu verringern oder um dessen geordnete Abwicklung und Umstrukturierung sicherzustellen; Art. 28 Abs. 8 DORA: Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
		unterstützen, richten Finanzunternehmen Ausstiegsstrategien ein. […] Finanzunternehmen stellen sicher, dass sie aus vertraglichen Vereinbarungen ausscheiden können, ohne: a) Unterbrechung ihrer Geschäftstätigkeit, b) Einschränkung der Einhaltung regulatorischer Anforderungen, c) Beeinträchtigung der Kontinuität und Qualität ihrer für Kunden erbrachten Dienstleistungen.				
F.8 - Festlegung eines Übergangszeitraums in der Ausstiegsstrategie	Der Vertrag muss eine Ausstiegsstrategie festlegen, die einen verbindlichen, angemessenen Übergangszeitraum umfasst. Dieser Zeitraum muss sicherstellen, dass dem Finanzunternehmen ausreichend Zeit für den Wechsel oder die Umstellung auf alternative Lösungen gegeben wird, die der Komplexität der erbrachten IKT-Dienstleistungen entsprechen.	Art. 30 Abs. 3 lit. f (ii, iii) DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: f) Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums, i) in dem der IKT-Drittdienstleister weiterhin die entsprechenden Funktionen oder IKT-Dienstleistungen bereitstellt, um das Risiko von Störungen im Finanzunternehmen zu verringern oder um dessen geordnete Abwicklung und Umstrukturierung sicherzustellen; ii) der dem Finanzunternehmen ermöglicht, zu einem anderen IKT-Drittdienstleister zu wechseln oder auf interne Lösungen umzustellen, die der Komplexität der erbrachten Dienstleistung entsprechen.			X	X
F.9 - Szenarien in Ausstiegsstrategien	Die Ausstiegsstrategie im Vertrag muss Szenarien berücksichtigen, die zu Störungen oder Risiken bei der Bereitstellung der IKT-Dienstleistungen führen können, einschließlich: • Fehler des IKT-Drittdienstleisters • Verschlechterung der Dienstleistungsqualität • Unterbrechung der Geschäftstätigkeit • Risiken bei der kontinuierlichen Bereitstellung der IKT-Dienstleistungen • Geplante oder ungeplante Beendigung der vertraglichen Vereinbarungen	Art. 28 Abs. 8 DORA: Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, richten Finanzunternehmen Ausstiegsstrategien ein. In den Ausstiegsstrategien wird den Risiken Rechnung getragen, die auf der Ebene der IKT-Drittdienstleister entstehen können, darunter insbesondere ein möglicher Fehler des IKT-Drittdienstleisters, eine Verschlechterung der Qualität der bereitgestellten IKT-Dienstleistungen, jede Unterbrechung der Geschäftstätigkeit aufgrund unangemessener oder unterlassener Bereitstellung von IKT-Dienstleistungen oder jedes erhebliche Risiko im Zusammenhang mit der angemessenen und kontinuierlichen Bereitstellung der jeweiligen IKT-Dienstleistungen oder der Beendigung vertraglicher Vereinbarungen mit IKT-Drittdienstleistern unter einem der in Absatz 7 genannten Umstände. […]			X	X
G: Bestimmungen zur Prüfung und Überwachung						
G.1 - Zusammenarbeit mit Behörden	Der Vertrag muss den IKT-Drittdienstleister verpflichten, uneingeschränkt mit den zuständigen Behörden des Finanzunternehmens, einschließlich der von diesen benannten Personen, zusammenzuarbeiten, beispielsweise bei Vor-Ort-Inspektionen sowie Audits.	Art. 30 Abs. 2 lit. g DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente: g) die Verpflichtung des IKT-Drittdienstleisters, vollumfänglich mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, einschließlich der von diesen benannten Personen; AT 9 Tz. 7 lit. l MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: i) Sicherstellung der uneingeschränkten Informations- und Prüfungsrechte sowie der Kontrollmöglichkeiten der gemäß § 25b Absatz 3 KWG zuständigen Behörden bezüglich der ausgelagerten Aktivitäten und Prozesse, Art. 3, Abs. 8 lit. c RTS TPPol: In der Leitlinie ist ausdrücklich festzulegen, dass die vertraglichen Vereinbarungen […] c) vorschreiben müssen, dass die IKT-Drittdienstleister mit den zuständigen Behörden zusammenarbeiten; Art. 30 Abs. 3 lit. e (iii) DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört: iii) die Verpflichtung des IKT-Drittdienstleisters zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, dem Finanzunternehmen oder einem beauftragten Dritten durchgeführt werden; und	X	X	X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
G.2 - Zugangsbestimmungen	Der Vertrag muss sicherstellen, dass das Finanzunternehmen, seine Revisoren und die zuständigen Behörden jederzeit wirksamen Zugang zu Daten und Räumlichkeiten haben, die mit der Nutzung von IKT-Dienstleistungen des Finanzunternehmens in Verbindung stehen. Zudem müssen Regelungen zu den Zugriffsberechtigungen auf Softwarelösungen festgelegt werden, die zum Schutz wesentlicher Daten und Informationen verwendet werden.	Art. 3 (8) (d) RTS TPPol In der Leitlinie ist ausdrücklich festzulegen, dass die vertraglichen Vereinbarungen […] d) vorschreiben müssen, dass das Finanzunternehmen, seine Revisoren und die zuständigen Behörden wirksam Zugang zu Daten und Räumlichkeiten haben müssen, die mit der Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zusammenhängen. AT 9 Tz. 7 lit. k MaRisk: […] Zu den sonstigen Sicherheitsanforderungen zählen vor allem Zugangsbestimmungen zu Räumen und Gebäuden (z. B. bei Rechenzentren) sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen..		X	X	X
G.3 - Recht auf fortlaufende Überwachung der IKT-Dienstleistung	Der Vertrag muss dem Finanzunternehmen das Recht einräumen, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, um sicherzustellen, dass die erbrachten IKT-Dienstleistungen den vereinbarten Standards und Anforderungen entsprechen.	Art. 30 Abs. 3 lit. e DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen [...] AT 9 Tz. 7 lit.k [...] Sonstigen Sicherheitsanforderungen [...]Die Einhaltung dieser Anforderungen ist fortlaufend zu überwachen. Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: h) Festlegung angemessener Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer. Informations- und Prüfungsrechte gem. Tz. 7 h) und i) umfassen auch die für den Zutritt, Zugang oder Zugriff erforderlichen Rechte.		X	X	X
G.4 - Uneingeschränkte Zugangs-, Inspektions- und Auditrechte	Der Vertrag muss dem Finanzunternehmen oder beauftragten Dritten das Recht auf die Durchführung von Inspektionen und Audits (ink. der Rechte für den Zutritt, Zugang oder Zugriff) gewähren.	Art. 30 Abs. 3 lit. e (i) DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört: i) uneingeschränkte Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten und der zuständigen Behörde […] Art. 28 Abs. 6 DORA: Bei der Ausübung der Zugangs-, Inspektions- und Auditrechte in Bezug auf den IKT-Drittdienstleister bestimmen Finanzunternehmen auf der Grundlage eines risikobasierten Ansatzes vorab die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche, indem allgemein anerkannte Auditstandards im Einklang mit etwaigen Aufsichtsanweisungen für die Anwendung und Einbeziehung solcher Auditstandards eingehalten werden. [...] Art. 8 Abs. 2 lit.a RTS TPPol: In der Leitlinie ist festzulegen, dass die einschlägigen vertraglichen Vereinbarungen das Recht des Finanzunternehmens auf Zugang zu Informationen, auf die Durchführung von Inspektionen und Audits sowie auf die Durchführung von IKT-Tests vorsehen müssen. In der Leitlinie ist vorzusehen, dass das Finanzunternehmen zu diesen Zwecken — unbeschadet seiner letztlichen Verantwortung — auf folgende Methoden zurückgreifen muss: a) eigene interne Audits oder Audits eines beauftragten Dritten; AT 9 Tz. 7 lit. h MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: h) Festlegung angemessener Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer, Informations- und Prüfungsrechte gem. Tz. 7 h) und i) umfassen auch die für den Zutritt, Zugang oder Zugriff erforderlichen Rechte.		X	X	X
G.5 - Vereinbarung über Umfang, Häufigkeit und Verfahren der Audits und Inspektionen	Der Vertrag muss Regelungen zu Umfang, Häufigkeit und Verfahren der Inspektionen und Audits beinhalten. Diese Regelungen müssen sicherstellen, dass das Finanzunternehmen die Inspektionen und Audits auf Grundlage eines risikobasierten Ansatzes und unter Einhaltung allgemein anerkannter Auditstandards und entsprechender Aufsichtsanweisungen durchführen kann.	Art. 30 Abs. 3 lit. e (iv) DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört: iv) die Verpflichtung, Einzelheiten zu Umfang und Häufigkeit dieser Inspektionen sowie dem dabei zu befolgenden Verfahren mitzuteilen; Art. 28 Abs. 6 DORA: Bei der Ausübung der Zugangs-, Inspektions- und Auditrechte in Bezug auf den IKT-Drittdienstleister bestimmen Finanzunternehmen auf der Grundlage eines risikobasierten Ansatzes vorab die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche, indem allgemein anerkannte Auditstandards im Einklang mit		X	X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
		etwaigen Aufsichtsanweisungen für die Anwendung und Einbeziehung solcher Auditstandards eingehalten werden. [...}				
G.6 - Recht auf Zugang zu Informationen	Der Vertrag muss dem Finanzunternehmen das Recht auf Zugang zu relevanten Informationen gewähren, die für die Überwachung und Kontrolle der erbrachten IKT-Dienstleistungen notwendig sind.	Art. 8 Abs. 2 RTS TPPol: In der Leitlinie ist festzulegen, dass die einschlägigen vertraglichen Vereinbarungen das Recht des Finanzunternehmens auf Zugang zu Informationen [...] vorsehen müssen AT 9 Tz. 7 lit. h MaRisk: 7 Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: h) Festlegung angemessener Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer, Art. 9 Abs. 2 lit. c RTS TPPol: […] Die Leitlinie muss insbesondere gewährleisten, dass c)das Finanzunternehmen andere relevante Informationen von den IKT-Drittdienstleistern erhält;		X	X	X
G.7 - Recht auf Anfertigung von Kopien relevanter Unterlagen	Der Vertrag muss dem Finanzunternehmen das Recht einräumen, Kopien von relevanten Unterlagen vor Ort anzufertigen, wenn diese für die Geschäftstätigkeit des IKT-Drittdienstleisters entscheidend sind.	Art. 30 Abs. 3 lit. e (i) DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört: i) […] das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort, wenn ihnen für die Geschäftstätigkeit des IKT-Drittdienstleisters entscheidende Bedeutung zukommt, wobei die tatsächliche Ausübung dieser Rechte nicht durch andere vertragliche Vereinbarungen oder Umsetzungsrichtlinien behindert oder eingeschränkt wird;			X	X
G.8 - Vereinbarungen zur Durchführung von unabhängigen Überprüfungen und Audits	Der Vertrag muss sicherstellen, dass unabhängige Überprüfung und Audits durchgeführt werden (sei es initiiert durch das Finanzunternehmen oder den IKT-Dienstleister), um die Einhaltung der rechtlichen und regulatorischen Anforderungen sowie der Strategien des Finanzunternehmens zu prüfen.	Art. 9 Abs. 2 lit. e RTS TPPol: In der Leitlinie wird festgelegt, wie das Finanzunternehmen bewertet, ob die IKT-Drittdienstleister, die für die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen in Anspruch genommen werden, angemessene Leistungs- und Qualitätsstandards im Einklang mit der vertraglichen Vereinbarung und den Strategien des Finanzunternehmens einhalten. Die Leitlinie muss insbesondere gewährleisten, dass [...] e) eine unabhängige Überprüfung und Audits vorgenommen werden, um die Einhaltung der rechtlichen und regulatorischen Anforderungen und Strategien zu prüfen.			X	X
G.9 - Recht zur Änderung des Umfangs von Zertifizierungen und Auditberichten	Der Vertrag muss dem Finanzunternehmen das Recht einräumen, Änderungen des Umfangs der Zertifizierungen oder Auditberichte mit Blick auf andere relevante Systeme und Kontrollen in einer für das Risikomanagement vertretbaren und legitimen Häufigkeit zu verlangen.	Art. 8 Abs. 3 lit. g RTS TPPol: Das Finanzunternehmen darf sich längerfristig nicht nur auf die in Absatz 2 Buchstabe c genannten Zertifizierungen oder die in Absatz 2 Buchstabe d genannten Auditberichte verlassen. Nach der Leitlinie ist die Anwendung der in Absatz 2 Buchstaben c und d genannten Methoden nur dann gestattet, wenn das Finanzunternehmen [...] g) das vertragliche Recht hat, in einer aus der Perspektive des Risikomanagements vertretbaren und legitimen Häufigkeit Änderungen des Umfangs der Zertifizierungen oder Auditberichte mit Blick auf andere einschlägige Systeme und Kontrollen zu verlangen;			X	X
G.10 - Recht auf Durchführung von Einzel- und Sammelaudits	Der Vertrag muss dem Finanzunternehmen das Recht einräumen, nach eigenem Ermessen Einzel- und Sammelaudits im Zusammenhang mit den vertraglichen Vereinbarungen durchzuführen und diese Rechte in der vereinbarten Häufigkeit wahrzunehmen.	Art. 8 Abs. 3 lit. h RTS TPPol: Das Finanzunternehmen darf sich längerfristig nicht nur auf die in Absatz 2 Buchstabe c genannten Zertifizierungen oder die in Absatz 2 Buchstabe d genannten Auditberichte verlassen. Nach der Leitlinie ist die Anwendung der in Absatz 2 Buchstaben c und d genannten Methoden nur dann gestattet, wenn das Finanzunternehmen h) das vertragliche Recht hat, nach eigenem Ermessen Einzel- und Sammelaudits im Zusammenhang mit den vertraglichen Vereinbarungen durchzuführen und diese Rechte in der vereinbarten Häufigkeit wahrzunehmen.			X	X
G.11 - Recht auf alternative Bestätigungsniveaus bei betroffenen Kundenrechten	Der Vertrag muss dem Finanzunternehmen das Recht einräumen, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen. Wenn die üblichen Auditrechte aufgrund der Rechte anderer Kunden des Dienstleisters zu Konflikten führen würden, muss das Finanzunternehmen die Möglichkeit haben, alternative Bestätigungsniveaus zu vereinbaren, um die Leistung des Dienstleisters weiterhin zu überwachen. Beispiel: Wenn ein Audit Zugriff auf sensible Kundendaten erfordert, kann eine stichprobenartige Prüfung der Systemleistung oder die Verwendung anonymisierter Daten vereinbart werden, um die Leistung ohne Konflikte mit den Datenschutzrechten anderer Kunden zu überwachen.	Art. 30 Abs. 3 lit. e (ii) DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes: e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört: ii) das Recht, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind;			X	X

Anforderung	Beschreibung	Auszüge aus den Rechtstexten				
G.12 - Weisungsrechte des Finanzunternehmens	Der Vertrag muss Weisungsrechte des Finanzunternehmens gegenüber dem IKT-Drittdienstleister festlegen, soweit dies erforderlich ist, um sicherzustellen, dass die erbrachten IKT-Dienstleistungen den vertraglichen Anforderungen entsprechen. Auf eine explizite Vereinbarung von Weisungsrechten kann verzichtet werden, wenn die zu erbringende Leistung hinreichend klar im Vertrag spezifiziert ist.	AT 9 Tz. 7 lit. j MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: j) soweit erforderlich Weisungsrechte, Weisungsrechte des Instituts/Prüfungen der Internen Revision Auf eine explizite Vereinbarung von Weisungsrechten zugunsten des Instituts kann verzichtet werden, wenn die vom Auslagerungsunternehmen zu erbringende Leistung hinreichend klar im Auslagerungsvertrag spezifiziert ist. Ferner kann die Interne Revision des auslagernden Instituts unter den Voraussetzungen von BT 2.1 Tz. 3 auf eigene Prüfungshandlungen verzichten. Diese Erleichterungen können auch bei Auslagerungen auf so genannte Mehrmandantendienstleister in Anspruch genommen werden.		X		X
H: Bestimmungen zum Berichtswesen						
H.1 - Vereinbarung zu Berichtspflichten bei Beeinträchtigung des Leistungsniveaus	Der Vertrag muss den IKT-Drittdienstleister verpflichten, dem Finanzunternehmen alle wesentlichen Entwicklungen zu melden, die die Erbringung der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus beeinträchtigen könnten.	Art. 30 Abs. 3 lit. b DORA: Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen […] Meldung aller Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters, IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus wirksam bereitzustellen, auswirken könnten; AT 9 Tz. 7 lit. n MaRisk: Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: n) Verpflichtung des Auslagerungsunternehmens, das Institut über Entwicklungen zu informieren, die die ordnungsgemäße Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen können,		X	X	X
H.2 - Vereinbarung zur Bereitstellung von Berichten über die Erbringung der IKT-Dienstleistungen	Der Vertrag muss den IKT-Drittdienstleister verpflichten, dem Finanzunternehmen Berichte über die Erbringung von IKT-Dienstleistungen zur Verfügung zu stellen, um sicherzustellen, dass die vereinbarten Leistungsstandards eingehalten werden.	Art. 9 Abs. 2 lit. a RTS TPPol: […] Die Leitlinie muss insbesondere gewährleisten, dass a) die IKT-Drittdienstleister dem Finanzunternehmen angemessene Berichte über ihre Tätigkeiten und Dienstleistungen vorlegen, darunter [...] Berichte über die Erbringung von Dienstleistungen,			X	X
H.3 - Vereinbarung zur Bereitstellung von Berichten über Maßnahmen und Tests zur Geschäftsfortführung	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister dem Finanzunternehmen Berichte über Maßnahmen und Tests zur Geschäftsfortführung bereitstellt, um die Resilienz der erbrachten IKT-Dienstleistungen und die Wiederherstellungsfähigkeit im Notfall zu gewährleisten.	Art. 9 Abs. 2 lit. a RTS TPPol: […] Die Leitlinie muss insbesondere gewährleisten, dass a) die IKT-Drittdienstleister dem Finanzunternehmen angemessene Berichte über ihre Tätigkeiten und Dienstleistungen vorlegen, darunter [...] Berichte über Maßnahmen und Tests zur Geschäftsfortführung			X	X
H.4 - Vereinbarung zur Bereitstellung von Berichten über IKT-Sicherheit	Der Vertrag muss den IKT-Drittdienstleister dazu verpflichten, dem Finanzunternehmen Berichte über die IKT-Sicherheit vorzulegen, um die Einhaltung von Sicherheitsstandards und die Schutzmaßnahmen für die IKT-Dienstleistungen sicherzustellen.	Art. 9 Abs. 2 lit. a RTS TPPol: […] Die Leitlinie muss insbesondere gewährleisten, dass a) die IKT-Drittdienstleister dem Finanzunternehmen angemessene Berichte über ihre Tätigkeiten und Dienstleistungen vorlegen, darunter [...] Berichte über die IKT-Sicherheit			X	X
H.5 - Vereinbarungen zur Bereitstellung von Audit-Berichten und Zertifizierungen	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister dem Finanzunternehmen relevante Berichte über interne oder von Dritten durchgeführte Audits zur Verfügung stellt. Zudem sind Vereinbarungen über die Bereitstellung von Zertifizierungen Dritter zu treffen, die die Qualität und Sicherheit der erbrachten IKT-Dienstleistungen bestätigen.	Art. 8 Abs. 2 lit c + d RTS TPPol: […] In der Leitlinie ist vorzusehen, dass das Finanzunternehmen zu diesen Zwecken — unbeschadet seiner letztlichen Verantwortung — auf folgende Methoden zurückgreifen muss: [...] c) gegebenenfalls Zertifizierungen Dritter; d) gegebenenfalls Berichte über interne oder von Dritten durchgeführte Audits, die vom IKT-Drittdienstleister zur Verfügung gestellt werden.			X	X
H.6 - Vereinbarungen über die Bereitstellung von Berichten der Unterauftragnehmer	Der Vertrag muss sicherstellen, dass der IKT-Drittdienstleister, sofern erforderlich, verpflichtet wird, dem Finanzunternehmen die Berichte von kwF-relevanten Unterauftragnehmern zur Verfügung zu stellen.	Art. 4 Abs. 1 lit. f RTS Subcon: In der vertraglichen Vereinbarung zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister wird festgelegt, [...] , f) dass der IKT-Drittdienstleister in seinem Vertrag mit seinen Unterauftragnehmern die Überwachungs- und Berichterstattungspflichten dieses Unterauftragnehmers gegenüber dem IKT-Drittdienstleister und, sofern vereinbart, gegenüber dem Finanzunternehmen festzulegen hat;			X	X
H.7 - Meldung von und Berichte zu IKT-Vorfällen durch den IKT-Dienstleister	Der Vertrag muss den IKT-Drittdienstleister verpflichten, das Finanzunternehmen über schwerwiegende IKT-Vorfälle und erhebliche Cyberbedrohungen zu informieren, die die erbrachten IKT-Dienstleistungen betreffen, damit das Finanzunternehmen seine Meldepflichten erfüllen kann.	Art. 9 Abs. 2 lit. a RTS TPPol: […] Die Leitlinie muss insbesondere gewährleisten, dass a) die IKT-Drittdienstleister dem Finanzunternehmen angemessene Berichte über ihre Tätigkeiten und Dienstleistungen vorlegen, darunter [...] Berichte über Vorfälle			X	X