

Unverbindliche Musterklauseln für Verträge betreffend Informations- und Kommunikationsdienstleistungen

Hinweis: Bei den folgenden unverbindlichen Musterklauseln handelt es sich nicht um einen vollständigen IKT-Vertrag. Die unverbindlichen Musterklauseln stellen vielmehr eine Hilfestellung des Verbandes für die Gestaltung einzelner wichtiger Regelungsbestandteile eines IKT-Vertrags dar. Die Musterklauseln sind nicht mit den Aufsichtsbehörden abgestimmt. Der Verband übernimmt keine Gewähr und Haftung für Vollständigkeit und Richtigkeit.

DORA = Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act)

RTS TPPol = Delegierte Verordnung (EU) 2024/1773; Technischer Regulierungsstandard zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden

RTS-E SUB = Entwurf Technischer Regulierungsstandard zur Spezifizierung der in Art. 30 Absatz 2 Buchstabe a genannten Aspekte, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss.

ITS Register = Durchführungsverordnung (EU) 2024/2956 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates im Hinblick auf Standardvorlagen für das Informationsregister

Regelungsinhalt		Unverb. Musterformulierung	Hinweise / Wechselwirkung Ausgliederung
DORA Level 1	RTS Level 2		
Kapitel 1 – Vorbemerkung			
Vorbemerkung [Optional] *		[Optional] Dem Auftragnehmer ist bewusst, dass der Auftraggeber versicherungsaufsichtsrechtlichen Anforderungen unterliegt. Dazu zählen insbesondere die Anforderungen des Versicherungsaufsichtsgesetzes („VAG“), die Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen („MaGo“), die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor („DORA“), die Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25.	-

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und Rückversicherungstätigkeit (Solvabilität II), die Delegierte Verordnung (EU) 2015/35 der Kommission vom 10. Oktober 2014 zur Ergänzung der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) sowie die von der European Insurance and Occupational Pensions Authority („EIOPA“) und der Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin“) erlassenen Rechtsakte. Dieser Rahmenvertrag und die auf seiner Grundlage abgeschlossenen Einzelvereinbarungen [unzutreffendes ggf. streichen/individuell anpassen] müssen die vorstehenden Anforderungen – so weit im Rahmen der vorliegenden Leistungspflichten einschlägig – beachten und einhalten.</p>	
<p>Vorbemerkung [Optional]</p>		<p>[Optional] Der Auftragnehmer gewährleistet, die Vertragsleistungen in voller Übereinstimmung mit allen rechtlichen, regulatorischen und behördlichen Bestimmungen sowie relevanter Rechtsprechung zu erbringen, die auf den Auftraggeber anwendbar sind und zum direkten Leistungsumfang des Auftragnehmers gehören, insbesondere in Übereinstimmung mit den §§ 23 ff. VAG, den MaGo, Art. 274 VO (EU) 2015/35 und des DORA einschließlich konkretisierender Delegierter Rechtsakte und Durchführungsrechtsakte in ihrer jeweils geltenden Fassung und allen einschlägigen Bestimmungen und Auslegungsentscheidungen der BaFin, der EIOPA oder ihren Rechtsnachfolgern oder sonstigen zuständigen Aufsichtsbehörden (diese Anforderungen insgesamt „rechtliche Bestimmungen“) [ggf. unternehmensindividuell anzupassen/ zu ergänzen]. Die Vertragsparteien werden sich dabei</p>	-

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>unterstützen, alle rechtlichen Bestimmungen einzuhalten.</p> <p>Die Vertragsparteien vereinbaren, dass die Auftragsvergabe von Vertragsleistungen auf den Auftragnehmer den Auftraggeber nicht in seiner Fähigkeit beeinträchtigen darf, die rechtlichen Bestimmungen einzuhalten. Der Auftragnehmer wird dem Auftraggeber ermöglichen, die Erbringung der Leistungen laufend zu überwachen und zu beurteilen, sodass notwendige Korrekturmaßnahmen sofort ergriffen werden können.</p>	
Kapitel 2 – Mindestanforderungen an alle IKT-Verträge			
<p>Art. 30 Absatz 1 Die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittdienstleisters werden eindeutig zugewiesen und schriftlich dargelegt. Der vollständige Vertrag umfasst die Vereinbarung über die Dienstleistungsgüte und wird in einem schriftlichen Dokument, das den Parteien in Papierform zur Verfügung steht, oder in einem Dokument in einem anderen herunterladbaren, dauerhaften und</p>		<p>[unternehmensindividuell zu ergänzen]</p>	<p>Neben den aufgelisteten vertraglichen Vorgaben können noch weitere, im Katalog von Art. 30 Absatz 2 DORA nicht explizit genannte Themen vertraglich zu regeln sein, etwa bezüglich zusätzlicher Informationspflichten.</p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

zugänglichen Format dokumentiert.			
<p>Art. 30 Absatz 2 lit. a) eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat, wobei anzugeben ist, 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</p>		<p>Der Auftragnehmer erbringt für den Auftraggeber die im Einzelnen [im Vertrag / in der Anlage bzw. Leistungsschein/SLA] näher bezeichnete/n Leistung/en inkl. Dienstleistungsgüte (einschließlich Aktualisierung und Überarbeitung) ab dem/in dem [im Vertrag / in der Anlage bzw. Leistungsschein/SLA] jeweils benannten Zeitpunkt/Zeitraum.</p> <p>[Bezüglich der Unterauftragsvergabe bei Unterstützung kritischer/wichtiger Funktionen wird auf Kapitel IV verwiesen. Im Übrigen unternehmensindividuell bzw. dienstleistungspezifisch zu ergänzen]</p>	<p>Es kann ratsam sein, bereits in dem Vertrag/dem SLA eine Zuordnung der konkreten Dienstleistung zu einer der in dem ITS zum Informationsregister genannten IKT-Servicekategorien vorzunehmen.</p>
<p>Art. 30 Absatz 2 lit. 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, einschließlich des</p>		<p>[Einzelvertragsebene] Die Durchführung der Leistungen sowie die Verarbeitung der Daten einschließlich der Speicherung erfolgt durch den Auftragnehmer und ggf. seine Unterauftragnehmer ausschließlich an den in der [Anlage X] aufgeführten Standorten (Regionen und/oder Länder).</p> <p>Der Auftraggeber ist [ggf. Frist] vorab mindestens in Textform zu informieren, wenn der Auftragnehmer oder sein Unterauftragnehmer eine Änderung dieser Standorte beabsichtigt.</p>	<p>Die Vertragsparteien können über eine Widerspruchslösung bei einem beabsichtigten Wechsel von EU bzw. EWR zu Nicht-EU bzw. Nicht-EWR-Speicherstandorten nachdenken. Sollte es hierdurch zu einer signifikanten Änderung der Risikoanalyse kommen, macht ein Kündigungsrecht Sinn.</p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>Speicherorts, sowie die Auflage für den IKT-Drittdienstleister, das Finanzunternehmen vorab zu benachrichtigen, wenn er eine Änderung dieser Standorte beabsichtigt;</p>			
<p>Art. 30 Abs. 2 lit. c) Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten;</p>		<p>Der Auftragnehmer ist verpflichtet, bei Durchführung der vertraglichen Leistungen den Schutz der Auftraggeberdaten [ggf. konkret zu spezifizieren] zu gewährleisten. [ggf. Verweis auf AV]</p> <p>Der Auftragnehmer wird bei der Erbringung der vertraglich geschuldeten Leistungen alle einschlägigen Gesetze und Vorschriften zum Schutz personenbezogener Daten beachten [ggf. auf AVV/TOMs/C2C-TOMs verweisen]. Um einen dem jeweils aktuellen Stand der Technik entsprechenden Schutz der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der sonstigen Auftraggeberdaten zu gewährleisten, wird der Auftragnehmer die in [Anlage X (TOMs)] beschriebenen Maßnahmen entsprechend umsetzen und während der Vertragslaufzeit aufrechterhalten. Der Auftragnehmer wird diese Maßnahmen kontinuierlich prüfen und bei Bedarf anpassen, um einen dem aktuellen Stand der Technik entsprechenden Schutz zu gewährleisten.</p> <p>Bei Verwendung von nicht seinem Zugriff unterliegenden Systemen, Komponenten und Prozessen hat der Auftragnehmer seinen Vertragspartnern entsprechende Verpflichtungen aufzuerlegen und deren Einhaltung regelmäßig zu überwachen. Dies beinhaltet auch die Verpflichtung Informationen gegenüber dem Auftraggeber</p>	<p>Hinweis: Informationen u.U. auch für das Informationsregister relevant.</p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		offenzulegen, welche dieser für eine erforderliche Risikoanalyse benötigt.	
<p>Art. 30 Absatz 2 lit. 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;</p>		<p>Im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des Auftragnehmers oder einer Beendigung der vertraglichen Vereinbarung bleibt der Auftragnehmer [zu den vertraglichen Konditionen] verpflichtet, solange Zugang zu personenbezogenen und nicht personenbezogenen Daten zu gewähren bis eine Wiederherstellung bzw. Rückgabe dieser Daten [nach Wahl des Auftraggebers statt Rückgabe Löschung] erfolgt ist [längstens jedoch X Monate].</p> <p>Die Rückgabe hat auf Anforderung in einem leicht zugänglichen, üblichen [vom Auftraggeber vorgegebenen] Format an den Auftraggeber oder an einen vom Auftraggeber benannten Dritten zu erfolgen. [Alternativ: Der Auftragnehmer sichert zu, dass in einem der oben genannten Fälle der Auftraggeber die Daten selbstständig oder mit Unterstützung des Auftragnehmers exportieren kann. Der vollständige Export wird dem Auftraggeber innerhalb von maximal XX Arbeitstagen zur Verfügung gestellt. Ein Zurückbehaltungsrecht kann gegen das Verlangen auf Export der Daten nicht geltend gemacht werden.]</p> <p>Nach erfolgreicher Rückgabe [oder als Alternative zur Rückgabe] hat der Auftragnehmer eventuell verbliebene Datenbestände des Auftraggebers nach dem aktuellen Stand der Technik unwiderruflich zu löschen und auf Verlangen des Auftraggebers einen Nachweis hierüber zu erbringen. [Dies gilt nicht, soweit und solange sich der Auftragnehmer auf einen Rechtsgrund für die fortgesetzte Speicherung berufen kann.]</p>	

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		[Optional] Sofern die Möglichkeit besteht, dass die Zugriffsmöglichkeit des Auftraggebers auf seine Daten beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet wird oder absehbar gefährdet werden könnte, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen und alles seinerseits Erforderliche zu tun, um die Zugriffsmöglichkeit des Auftraggebers sicherzustellen. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen und Beteiligten unverzüglich darüber informieren, dass die (Entscheidungs-)Hoheit über die Daten ausschließlich beim Auftraggeber liegt.	
Art. 30 Absatz 2 lit. e) Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen;		[Unternehmens- bzw. dienstleistungsspezifisch zu ergänzen]	
Art. 30 Abs. 2 lit. 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;		Der Auftragnehmer ist verpflichtet, dem Auftraggeber bei einem IKT-Vorfall, der mit der für den Auftraggeber bereitgestellten IKT-Dienstleistung in Verbindung steht, Unterstützung zu leisten. Der Auftragnehmer wird die Unterstützungsleistungen ohne zusätzliche Vergütung erbringen / zu folgenden Konditionen erbringen [unzutreffendes streichen und individuell anpassen]	

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>Art. 30 Abs. 2 lit. g) die Verpflichtung des IKT-Drittdienstleisters, vollumfänglich mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, einschließlich der von diesen benannten Personen;</p>		<p>Der Auftragnehmer verpflichtet sich, mit den für den Auftraggeber zuständigen Behörden, insbesondere auch mit den Aufsichts- und Abwicklungsbehörden, einschließlich weiterer von diesen benannten Personen, vollumfänglich zusammenzuarbeiten.</p>	
<p>Art. 30 Abs. 2 lit. h) Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und der Abwicklungsbehörden;</p> <p>Art. 28 Abs. 7</p> <p>Art. 31 Abs. 12</p>		<p>Der Auftraggeber [beide Parteien] hat [haben] das Recht zur außerordentlichen Kündigung aus wichtigem Grund.</p> <p>Die Parteien sind sich darüber einig, dass insbesondere bei Vorliegen folgender Umstände der Auftraggeber zur außerordentlichen Kündigung aus wichtigem Grund berechtigt ist:</p> <p>a) ein erheblicher Verstoß des Auftragnehmers [und/oder seiner Unterauftragnehmer] gegen geltende Gesetze, sonstige Vorschriften oder Bedingungen dieses Vertrages;</p> <p>b) Umstände, die im Laufe der Überwachung des IKT-Drittparteienrisikos im Sinne von Art. 3 Nr. 18 der Verordnung (EU) 2022/2554 festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen und IKT-Dienstleistungen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des Auftragnehmers auswirken (z.B. Change of Control);</p>	

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>c) nachweisliche Schwächen des Auftragnehmers 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;</p> <p>d) die zuständige Behörde kann den Auftraggeber [bzw. dessen Auftraggeber/das Finanzunternehmen] infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen. Klarstellend wird festgehalten, dass dieser Umstand erst vorliegt, wenn die Behörde eine Beendigung der vertraglichen Vereinbarung oder eine Änderung verlangt, auf welche sich die Parteien nicht einigen können;</p> <p>e) Die Vermögensverhältnisse des Auftragnehmers verschlechtern sich wesentlich und dem Auftraggeber ist daher das Festhalten an diesem Vertrag nicht zumutbar;</p> <p>f) Der Auftragnehmer hat seinen Sitz außerhalb der EU, wurde als kritisch im Sinne von Artikel 31 Absatz 1 Buchstabe a der VO (EU) 2022/2554 eingestuft, und hat weder ein Tochterunternehmen in der Union noch beabsichtigt er dieses innerhalb von 12 Monaten nach der Einstufung als kritisch zu gründen;</p>	
--	--	---	--

		g) sonstige Umstände, welche zu einer aus Sicht des Auftraggebers untragbaren Risikoerhöhung führen würden. [Kündigungsfristen unternehmensindividuell zu ergänzen]	
Art. 30 Abs. 2 lit. 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.		[Die Bedingungen sind unternehmensindividuell zu gestalten] Beide Parteien sichern sich gegenseitig zu, dass sie ihr in die Leistungserbringung involviertes Personal im erforderlichen Umfang mit Blick auf die IKT-Sicherheit sensibilisieren und das Wissen durch Schulungen im erforderlichen Umfang aktuell halten. Der Auftraggeber bietet zu diesem Zweck Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz an (gemeinsam: IKT-Qualifizierung). Auf Anforderung des Auftraggebers weist der Auftragnehmer das von ihm zur vertraglich geschuldeten Leistungserbringung eingesetzte Personal an, an einer IKT-Qualifizierung des Auftraggebers [ggf. externe Anbieter ergänzen] teilzunehmen. Eine Anforderung kann der Auftragnehmer nur zurückweisen, wenn er nachweist, dass das eingesetzte Personal in den vergangenen XX Monaten an einer IKT-Qualifizierung mit vergleichbarem Inhalt teilgenommen hat. Einzelheiten zum Umfang und zur Durchführung der IKT-Qualifizierung werden die Parteien innerhalb von XX Wochen nach Anforderung regeln.	Konsistenz zu internen Schulungsvorgaben sollte gegeben sein. Gegebenenfalls können Regelungen zu etwaigen Kostenerstattungen im Zusammenhang mit den Schulungen (etwa Fahrtkosten) sinnvoll sein.
Vorfallsmeldungen		Der Auftragnehmer meldet IKT-bezogene Vorfälle iSd Art. 3 Nr. 8 DORA an den Auftraggeber, soweit diese sich auf die geschuldete IKT-Dienstleistung auswirken können. Ebenso meldet er erhebliche	In der Anlage X kann ggf. auch eine Vorklassifizierung durch den Dienstleister geregelt werden.

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		Cyberbedrohungen iSd Art. 3 Nr. 13 DORA, soweit diese die geschuldete IKT-Dienstleistung bedrohen können. Meldefrist, Inhalt der konkreten Meldung und das Meldeverfahren wurden zwischen den Parteien auf Basis des Prozesses gemäß Art. 17 DORA abgestimmt und in Anlage X dokumentiert.	
Kapitel 3 – Zusätzliche Anforderungen bei der Unterstützung kritischer/wichtiger Funktionen oder wesentlicher Teile davon			
	Art. 8 Abs. 4 RTS TPPol		Wesentliche Änderungen der vertraglichen Vereinbarung werden in einem schriftlichen Dokument förmlich festgehalten, das von allen Parteien datiert und unterzeichnet wird und in dem das Verfahren zur Verlängerung der vertraglichen Vereinbarung festgelegt ist.
Art. 30 Absatz 3 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	Art. 9 Abs. 1 und 2 RTS TPPol	Der Auftragnehmer erbringt für den Auftraggeber die im Einzelnen [im Vertrag / in der Anlage zum Vertrag bzw. im Leistungsschein/Service-Level-Agreement (SLA)] näher bezeichnete/n Leistung/en in der dort beschriebenen Leistungsqualität (Dienstleistungsgüte), deren Einhaltung durch die Vereinbarung quantitativer und qualitativer Leistungsziele gewährleistet wird. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, die Leistung des Auftragnehmers laufend zu überwachen, um auch das unverzügliche Ergreifen angemessener Korrekturmaßnahmen zur Wiederherstellung der vereinbarten Dienstleistungsgüte zu ermöglichen, wenn diese nicht erreicht wird. Zur Ermöglichung der laufenden Überwachung der vereinbarten Leistungsziele verpflichtet sich der Auftragnehmer zur Erstellung und Übersendung eines	Bei wesentlichen Ausgliederungen ggf. an Weisungsbefugnis denken (Art. 274 Abs. 4 lit. f) VO (EU) 2015/35)

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>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;</p>		<p>Berichts an den Auftraggeber. Die Form und das Intervall des Reportings sind [in der Anlage X] geregelt. Aktualisierungen oder Überarbeitungen der Leistungsqualität (Dienstleistungsgüte) sind durch eine entsprechende Änderung [im Vertrag / in der Anlage zum Vertrag bzw. im Leistungsschein/Service-Level-Agreement (SLA)] zu vereinbaren.</p> <p>[ggf. unternehmensindividuell Maßnahmen und Schlüsselindikatoren zur Überwachung der Leistungsfähigkeit zu ergänzen]</p> <p>[Optional] Für die vertragliche und administrative Koordination der Zusammenarbeit benennen beide Vertragsparteien je einen verantwortlichen Ansprechpartner. Die Vertragsparteien stimmen sich in regelmäßigem Zyklus über die Qualität der Leistungserbringung, über Problemfälle sowie anstehende Änderungen des Leistungsumfangs (Aktualisierungen und Überarbeitungen) ab. Beide Vertragsparteien sind zur Teilnahme an entsprechenden Treffen verpflichtet.</p>	
	<p>Art. 9 Absatz 1 RTS TPPoI</p>	<p>[ggf. unternehmensindividuell Folgen bei Nichterreichung der vereinbarten Dienstleistungsgüte vertraglich vereinbaren]</p>	<p>Kann ggf. bereits in obiger Klausel zur Dienstleistungsgüte ergänzt werden</p>
<p>Art. 30 Absatz 3 lit. b) Kündigungsfristen und Berichtspflichten des IKT-Drittdienstleisters gegenüber dem Finanzunternehmen, einschließlich der Meldung aller Entwicklungen, die sich</p>	<p>Art. 9 Absatz 2 RTS TPPoI</p>	<p>Der Auftragnehmer legt dem Auftraggeber regelmäßig angemessene Berichte über seine Tätigkeit und Dienstleistungen sowie Berichte über Vorfälle, einschließlich operationaler oder sicherheitsbezogener Vorfälle im Zusammenhang mit Zahlungen, die IKT-Sicherheit und über Maßnahmen und Tests zur Geschäftsfortführung vor. Insbesondere berichtet der Auftragnehmer dem Auftraggeber unverzüglich über alle Entwicklungen, die sich wesentlich auf seine</p>	<p>Alternativ kann zur laufenden Überwachung auch eine einheitliche Klausel – bestehend aus den Reportingpflichten in voriger Klausel und dieser Klausel gewählt werden, beispielsweise: <i>“Zur Ermöglichung der laufenden Überwachung der</i></p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>wesentlich auf die Fähigkeit des IKT-Drittdienstleisters, IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus wirksam bereitzustellen, auswirken könnten;</p>		<p>Fähigkeit, IKT-Dienstleistungen gemäß den vereinbarten Leistungsniveaus wirksam bereitzustellen, auswirken könnten, einschließlich IKT-bezogener Vorfälle und operationaler oder sicherheitsbezogener Vorfälle im Zusammenhang mit Zahlungen. [Kündigungsfristen bzw. Beendigungsbedingungen individuell im Einklang mit Artikel 10 RTS TPPol zu ergänzen]</p>	<p><i>Dienstleistungsgüte anhand der vereinbarten Leistungsziele und zur Ermöglichung der Risikosteuerung erstellt und übersendet der Auftragnehmer Berichte an den Auftraggeber (z. B. Berichte über Vorfälle, über die Erbringung von Dienstleistungen, über die IKT-Sicherheit und über Maßnahmen und Tests zur Geschäftsfortführung). Insbesondere meldet der Auftragnehmer dem Auftraggeber unverzüglich alle Entwicklungen, die sich wesentlich auf seine Fähigkeit, IKT-Dienstleistungen gemäß den vereinbarten Absprachen bereitzustellen, auswirken könnten, einschließlich IKT-bezogener Vorfälle und operationaler oder sicherheitsbezogener Vorfälle im Zusammenhang mit Zahlungen. Form, Inhalt, Adressaten und Intervall des Reportings sind [in der Anlage X] geregelt."</i></p>
<p>Art. 30 Absatz 3 lit. c) Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen und über</p>		<p>Der Auftragnehmer implementiert und testet Notfallpläne und verfügt über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch den Auftraggeber im Einklang mit seinem Rechtsrahmen bieten.</p>	

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>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;</p>		<p>[ggf. unternehmens- bzw. dienstleistungsspezifisch zu konkretisieren]</p>	
<p>Art. 30 Absatz 3 lit. d) die Verpflichtung des IKT-Drittdienstleisters, sich an den in den Artikeln 26 und 27 genannten TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken;</p>		<p>Der Auftragnehmer ist verpflichtet, sich an den bedrohungsorientierten Penetrationstests des Auftraggebers (TLPT — Threat-Led Penetration Testing) gemäß der Verordnung (EU) 2022/2554 (DORA) zu beteiligen und uneingeschränkt daran mitzuwirken.</p> <p>Die zuständigen Behörden ermitteln Finanzunternehmen, die TLPT durchzuführen haben, unter Berücksichtigung der in Artikel 4 Absatz 2 der DORA-Verordnung aufgeführten Kriterien.</p> <p>[Optional]</p> <p>Für die Durchführung der bedrohungsorientierten Penetrationstests gelten folgende Regelungen:</p> <ul style="list-style-type: none"> a) Sie finden in der Regel mindestens alle drei (3) Jahre statt, es sei denn, für den Auftraggeber geltende gesetzliche Anforderungen oder Anordnungen durch Aufsichtsbehörden schreiben etwas anderes vor; b) Der Auftragnehmer wendet wirksame Risikomanagementkontrollen an, um die Gefahr potenzieller Auswirkungen auf Daten, Schäden 	<p>Es kann sinnvoll sein zu regeln, was passiert, wenn Daten verloren gehen bei der Live Attacke.</p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>an Vermögenswerten und Unterbrechung kritischer oder wichtiger Funktionen, Dienste oder Vorgänge zu mindern;</p> <p>c) Der Auftragnehmer unternimmt angemessene Maßnahmen zur Sicherung der Einhaltung des [SLA] in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten von Dritten, einschließlich des Schutzes personenbezogener Daten;</p> <p>d) Der Auftraggeber und die durch den Auftraggeber beauftragten Tester werden zur Dokumentation Abbildungen und/oder Vervielfältigungen der zur Kenntnis gelangenden Daten und Informationen anfertigen,;</p> <p>e) [ggf. Hinweis auf Vertraulichkeit]</p> <p>Für die zur Durchführung der bedrohungsorientierten Penetrationstests beauftragten Tester gelten folgende Anforderungen:</p> <p>a) Sie sind von höchster Eignung und Ansehen;</p> <p>b) Sie verfügen über technische und organisatorische Fähigkeiten und weisen spezifisches Fachwissen in den Bereichen Bedrohungsanalyse, Penetrationstests und Red-Team-Tests nach;</p> <p>c) Sie sind von einer Akkreditierungsstelle in einem Mitgliedstaat der Europäischen Union zertifiziert oder halten formale Verhaltenskodizes oder ethische Rahmenregelungen ein;</p> <p>d) Sie legen eine unabhängige Gewähr oder einen Auditbericht in Bezug auf das zuverlässige Management von Risiken vor, die mit der Durchführung von bedrohungsorientierten Penetrationstests verbunden sind, darunter</p>	
--	--	---	--

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>auch der angemessene Schutz vertraulicher Informationen und ein Ausgleich der geschäftlichen Risiken von Auftragnehmer und Auftraggeber;</p> <p>e) Sie sind ordnungsgemäß und vollständig durch einschlägige Berufshaftpflichtversicherungen abgesichert, einschließlich einer Versicherung gegen das Risiko von Fehlverhalten und Fahrlässigkeit.</p>	
<p>Art. 26 Abs. 4</p>		<p>[Optional] Der Auftragnehmer ist berechtigt, vertragliche Vereinbarungen mit einem externen Tester zu schließen, um unter der Leitung eines von ihm benannten und den aufsichtsrechtlichen Anforderungen der Verordnung (EU) 2022/2554 unterliegenden Finanzunternehmens einen gebündelten bedrohungsorientierten Penetrationstest durchzuführen, an denen mehrere diesen aufsichtsrechtlichen Anforderungen unterliegende Finanzunternehmen beteiligt sind, für die der Auftragnehmer Dienstleistungen erbringt („Gebündelter Test“), wenn vernünftigerweise davon auszugehen ist,</p> <p>a) dass sich der bedrohungsorientierte Penetrationstest nachteilig auf die Qualität oder die Sicherheit von Dienstleistungen auswirkt, die der Auftragnehmer gegenüber anderen, nicht den aufsichtsrechtlichen Anforderungen der Verordnung (EU) 2022/2554 unterliegenden Unternehmen erbringt; oder</p> <p>b) dass sich der bedrohungsorientierte Penetrationstest nachteilig auf die Vertraulichkeit in Bezug auf die mit diesen Dienstleistungen verbundenen Daten auswirkt.</p> <p>Bei einer Durchführung gebündelter Tests hat der Auftragnehmer die vertraglichen Vereinbarungen mit</p>	

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		dem externen Tester so auszugestalten, dass der Auftraggeber die aufsichtsrechtlichen und datenschutzrechtlichen Anforderungen einhalten kann und die entsprechenden Vereinbarungen im Einklang mit diesem Rahmenvertrag und/oder den Einzelvereinbarungen und/oder den Anlagen, insbesondere dem Inhalt und Umfang der Anlage X stehen.	
--	--	---	--

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>Art. 30 Absatz 3 lit. e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört:</p> <p>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;</p> <p>ii) das Recht, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind;</p>	<p>Art. 3 Absatz 8 und Artikel 8 Absatz 2 und 3 lit. c und g; Art. 9 Absatz 1 RTS TPPol</p>	<p>Der Auftraggeber hat das Recht, die Leistung des Auftragnehmers fortlaufend zu überwachen. Dazu gehört insbesondere:</p> <p>a) Der Auftraggeber hat das Recht auf IKT-Tests und wirksamen Zugang zu Räumlichkeiten und Informationen, welche im Zusammenhang mit der erbrachten IKT-Dienstleistung stehen.</p> <p>b) Der Auftraggeber einschließlich dessen zentralem Auslagerungsmanagement, Innenrevision, Datenschutzbeauftragten, Compliance-Beauftragten, ein von ihm oder den zuständigen Aufsichtsbehörden beauftragter Dritter, Wirtschaftsprüfer und die zuständigen Behörden haben uneingeschränkte Zugangs-, Inspektions- und Auditrechte, einschließlich Sammelaudits, sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort, wenn ihnen für die Geschäftstätigkeit des IKT-Drittdienstleisters entscheidende Bedeutung zukommt. Vereinbarungen, Umsetzungsrichtlinien oder interne Vorgaben des Auftragnehmers, die die tatsächliche Ausübung dieser Rechte behindern oder einschränken, sind unwirksam.</p> <p>c) Der Auftraggeber hat das Recht, sich auf eine andere Art und Weise als über die vereinbarten Zugangs-, Inspektions- und Auditrechte darüber zu versichern, dass die mit dem Auftragnehmer getroffenen Vereinbarungen eingehalten werden, wenn die Rechte anderer Kunden betroffen sind (alternatives Bestätigungsniveau).</p>	
--	---	--	--

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>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</p> <p>iv) die Verpflichtung, Einzelheiten zu Umfang und Häufigkeit dieser Inspektionen sowie dem dabei zu befolgenden Verfahren mitzuteilen;</p> <p>Hierzu auch Artikel 28 Absatz 6 (Vorabfestlegung der Häufigkeit von Audits und Inspektionen)</p>		<p>d) Der Auftragnehmer verpflichtet sich zur uneingeschränkten Zusammenarbeit mit den zuständigen Behörden, insbesondere bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, dem Auftraggeber oder einem beauftragten Dritten durchgeführt werden.</p> <p>e) Bzgl. Umfang und Häufigkeit der Inspektionen und Audits sowie dem dabei zu befolgenden Verfahren, sind sich die Parteien über Folgendes einig: [basierend auf Ergebnissen zu Art. 28 Abs. 6; ggf. Anlage - individuell zu ergänzen]</p> <p>f) [Sofern Zertifizierungen Dritter bzw. externe Audits genutzt werden sollen]: Der Auftraggeber hat das Recht in risikogerechter Häufigkeit Änderungen des Umfangs der Zertifizierungen oder Auditberichte mit Blick auf andere einschlägige Systeme und Kontrollen zu verlangen. Zudem hat er das Recht X-mal im Jahr nach eigenem Ermessen Einzel- und Sammelaudits im Zusammenhang mit den vertraglichen Vereinbarungen durchzuführen.</p> <p>g) [Die konkreten Maßnahmen und Schlüsselindikatoren zur Überwachung der Leistungsfähigkeit des Dienstleisters einschließlich Maßnahmen, welche dazu dienen die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Daten und Informationen und die Einhaltung der</p>	
--	--	---	--

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>einschlägigen Strategien und Verfahrens des VU durch den DL zu überwachen sind vertraglich festzulegen.]</p> <p>[ggf. unternehmensindividuell ergänzen]</p>	
--	--	--	--

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>Art. 30 Absatz 3 lit. f) Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums,</p>			<p>Es kann sinnvoll sein, auf einen Anhang hinsichtlich konkreter Rahmenparameter für den Ausstieg zu verweisen.</p>
<p>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;</p>		<p>Im Falle einer ganz oder teilweisen Beendigung des Vertrages durch eine der Vertragsparteien, sei es durch Kündigung oder durch Rücktritt, wird der Auftragnehmer nach einseitiger Erklärung des Auftraggebers die Leistungserbringung zu den vertraglichen Bedingungen insbesondere hinsichtlich der Einhaltung regulatorischer Anforderungen und der Kontinuität und Qualität der Dienstleistungen, bis zu XX Monate fortsetzen.</p>	<p>Hinweis: Ggf. nicht allein ausreichend, um reibungslosen Übergang zu ermöglichen.</p>
<p>ii) der dem Finanzunternehmen ermöglicht, zu einem anderen IKT- Drittdienstleister zu wechseln oder auf interne Lösungen umzustellen, die der Komplexität der erbrachten Dienstleistung entsprechen.</p>		<p>Im Falle einer ganz oder teilweisen Beendigung des Vertrages durch eine Vertragspartei, sei es durch Kündigung oder durch Rücktritt, wird der Auftragnehmer darüber hinaus eine Übertragung der vereinbarten Leistungen an ein anderes Unternehmen oder zurück zum Auftraggeber ermöglichen. Er wird den Auftraggeber dabei unterstützen, Unterbrechungen, Störungen oder sonstige Beeinträchtigungen des Geschäftsbetriebs des Auftraggebers bei der Übertragung der Leistungen an ein anderes Unternehmen oder zurück zum Auftraggeber zu vermeiden.</p>	
<p>Abweichend von Buchstabe e können der</p>			

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

<p>IKT-Drittdienstleister und das Finanzunternehmen, das ein Kleinstunternehmen ist, vereinbaren, dass die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens auf einen unabhängigen Dritten übertragen werden können, der vom IKT-Drittdienstleister benannt wird, sowie dass das Finanzunternehmen von diesem Dritten jederzeit Informationen und Gewähr in Bezug auf die Leistung des IKT-Drittdienstleisters verlangen kann.</p>			
<p>Kapitel 4 - Bedingungen Unterauftragsvergabe bei Unterstützung kritischer/wichtiger Funktion bzw. wesentlicher Teile davon</p>			
<p>Art. 30 Abs. 2 lit. a</p>		<p>Variante Zustimmung</p> <p>Der Auftragnehmer darf die übernommene Tätigkeit durch schriftlichen Vertrag (Textform ist ausreichend) ganz oder teilweise unterbeauftragen (Fremdbezug oder Unterauslagerung), wenn er dies dem Auftraggeber [ggf. mindestens XX Wochen - der Zeitraum ist individuell festzulegen] zuvor schriftlich (Textform ist ausreichend) anzeigt und der Auftraggeber daraufhin schriftlich (Textform ist ausreichend) zustimmt.</p>	<p>Hinweis: Die Bedingungen bzw. Entscheidung über Unterauftragsvergaben sind innerhalb der allgemeinen aufsichtsrechtlichen Regelungen und Konkretisierungen durch DORA bzw. den RTS-E SUB grundsätzlich frei. Um eine erste Orientierung zu bieten, sind diesem Kapitel Formulierungen für die Varianten "Zustimmung"</p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>[Optional]: Der Auftraggeber ist vor Vollzug der schriftlich genehmigten Unterbeauftragung von Dritten zu informieren.</p> <p>Dem Auftraggeber ist bekannt, dass der Auftragnehmer derzeit bereits [Name/Anschrift des/der Unterauftragnehmer und ausgeübte Tätigkeit - oder Verweis auf eine entsprechende Vertragsanlage] in vorgenanntem Sinne eingeschaltet hat.</p>	<p>(inklusive dem optionalen Zusatzbaustein “Widerruf der Zustimmung”) und eine “Widerspruchslösung” vorangestellt. Diese Möglichkeiten sind nicht abschließend.</p> <p>Eine detailliertere Formulierung, unter Einbeziehung einzelner Bausteine der nachfolgenden Anforderungen aus dem RTS-Entwurf zur Unterauftragsvergabe finden sich am Ende dieses Kapitels.</p>
		<p>[Optional] Widerruf Zustimmung</p> <p>Der Auftraggeber hat auch nach erteilter Zustimmung jederzeit das Recht, diese aus wichtigen Gründen zu widerrufen. Als wichtiger Grund gilt insbesondere, wenn</p> <ol style="list-style-type: none"> a. begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung ordnungsgemäß erbringt, b. die Geltendmachung der vorgenannten Rechte nicht sichergestellt ist, c. die zuständige Aufsichtsbehörde der Unterbeauftragung widerspricht, d. der Unterauftragnehmer seinen Sitz außerhalb der [EU/EWR] oder kundenbezogene Datenverarbeitung außerhalb der [EU/EWR] verlegt, e. durch die Unterbeauftragung einer Tätigkeit die Wirksamkeit der Beaufsichtigung dieser Tätigkeit durch 	<p>Widerruf als milderer Mittel vor der – ansonsten weiterhin möglichen – Kündigung.</p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>den Auftraggeber in irgendeiner Weise beeinträchtigt wird,</p> <p>f. der Unterauftragnehmer nicht über ausreichende Ressourcen, Kenntnisse und Erfahrung für die Ausführung der jeweiligen Aufgaben verfügt oder</p> <p>g. die zuständige Aufsichtsbehörde daran gehindert wird zu kontrollieren, dass der Auftraggeber seine gesetzlichen Verpflichtungen einhält.</p>	
		<p>Variante Widerspruch</p> <p>Der Auftragnehmer ist nur dann berechtigt, die übernommene Tätigkeit durch schriftlichen Vertrag (Textform ist ausreichend) ganz oder teilweise unterzubeauftragen (Fremdbezug oder Unterauslagerung), wenn der Auftraggeber nicht binnen [XX Wochen - der Zeitraum ist je nach Unternehmen individuell festzulegen] nach vollständiger Information über die geplante Unterauftragsvergabe einer solchen widerspricht.</p>	
	<p>Art. 4a und b RTS-E SUB</p>	<p>Der Auftragnehmer ist verpflichtet alle unterbeauftragten IKT-Dienstleistungen, welche im Zusammenhang mit der für den Auftraggeber zu erbringenden IKT-Dienstleistung stehen, fortlaufend zu überwachen, um sicherzustellen, dass seine vertraglichen Verpflichtungen gegenüber dem Auftraggeber fortlaufend eingehalten werden. Er bleibt gegenüber dem Auftraggeber für die Erbringung der vereinbarten Dienstleistungen durch Unterauftragnehmer verantwortlich.</p>	
	<p>Art. 4c RTS-E SUB</p>	<p>Werden in dem Überwachungsprozess Schwachstellen, Mängel oder Vorfälle bei dem Unterauftragnehmer festgestellt, so hat der Auftragnehmer den Auftraggeber</p>	<p>Im Zusammenhang mit der vorigen Klausel (zu Art. 4a und b RTS-E SUB) zu lesen.</p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		hierüber unverzüglich unter Vorlage der Ergebnisse in Textform zu informieren.	
	Art. 4d RTS-E SUB	Vor der Unterbeauftragung sowie fortlaufend hat der Auftragnehmer alle Risiken der Unterauftragsvergabe, einschließlich IKT-Risiken, zu bewerten, welche sich aus dem Standort des Unterauftragnehmers, dessen Muttergesellschaft und dem Standort der tatsächlichen Dienstleistungserbringung im konkreten Fall ergeben. Die Ergebnisse dieser Prüfung sind dem Auftraggeber vorzulegen.	Detailgrad und Intervall können je nach Dienstleister und unterstützter Funktion variieren.
	Art. 4e RTS-E SUB	[Falls zutreffend]	Hinweis: u.U. deckt die Klausel zu Art. 30 Abs. 2 lit. b) das bereits ab.
	Art. 4f RTS-E SUB	Der Auftragnehmer hat im Verhältnis zum Unterauftragnehmer die Überwachungs- und Berichtspflichten gegenüber dem Auftragnehmer [und ggf. Auftraggeber] in einer schriftlichen Vereinbarung zu spezifizieren. Diese müssen dem Risiko der Unterauftragsvergabe angemessen und derart gestaltet sein, dass der Auftragnehmer seinen Überwachungs- und Berichtspflichten gegenüber dem Auftraggeber gerecht werden kann.	
	Art. 4g RTS-E SUB	Der Auftragnehmer stellt sicher, dass die für den Auftraggeber zu erbringende Dienstleistung in der gesamten Auftragskette auch dann fortlaufend erbracht werden kann, wenn der Unterauftragnehmer seine vertraglich vereinbarte Dienstleistungsgüte nicht erreicht. In der schriftlichen Vereinbarung zwischen dem Auftragnehmer und dem Unterauftragnehmer werden die Implementierung und Testung von Notfallplänen vereinbart sowie die jeweilige Dienstleistungsgüte in Bezug auf diese Pläne definiert. Der Auftragnehmer stellt sicher, dass die Notfallpläne mit den im Verhältnis zwischen Auftraggeber und Auftragnehmer vereinbarten Notfallplänen harmonisieren.	Hinweis: Dienstleistungsgüte ist die offizielle Übersetzung in dem RTS. Gemeint sind insbesondere Service Levels. U.U. ist nach Bedarf eine Anlage mit Begriffserklärungen sinnvoll. Notfallpläne sind Thema von Art. 30 Abs. 3 lit. c – ggf. Harmonisierung erforderlich

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

	Art. 4h RTS-E SUB	Der Auftragnehmer stellt in einer schriftlichen Vereinbarung sicher, dass der Unterauftragnehmer über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit verfügt, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch den Auftraggeber im Einklang mit seinem Rechtsrahmen bieten.	Hinweis: Sicherheitsstandards sind Thema von Art. 30 Abs. 3 lit. c – ggf. Harmonisierung erforderlich.
	Art. 4i RTS-E SUB	Der Auftragnehmer stellt sicher, dass der Auftraggeber, dessen Aufsichts- und Abwicklungsbehörde sowie von diesen benannte Personen zumindest in demselben Umfang unmittelbare Audit-, Zugangs- und Inspektionsrechte gegenüber dem Unterauftragnehmer haben, wie diese im Verhältnis zwischen Auftraggeber und Auftragnehmer vereinbart wurden.	
	Art. 4k RTS-E SUB	<p>Unbeschadet weiterer Kündigungsrechte steht dem Auftraggeber ein Kündigungsrecht in folgenden Fällen zu:</p> <ul style="list-style-type: none"> a) die erbrachte Dienstleistung entspricht nicht der mit dem Auftraggeber vereinbarten Dienstleistungsgüte b) der Auftragnehmer nimmt trotz Ablehnung und Änderungsersuchen oder fehlender Zustimmung (ggf. unzutreffendes streichen) des Auftraggebers oder vor Ablauf der Prüffrist ohne Zustimmung wesentliche Änderungen an der Unterauftragsvergabe vor, einschließlich der Neubeauftragung eines Unterauftragnehmers. c) [optional] Der Auftragnehmer hält an einer Unterbeauftragung trotz Widerrufs der Zustimmung fest. d) der Auftragnehmer beauftragt einen Unterauftragnehmer für eine wichtige oder 	

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>kritische Funktion unterstützende Dienstleistung, für welche die vertragliche Vereinbarung keine ausdrückliche Unterauftragsvergabemöglichkeit vorsieht-</p> <p>e) der Auftragnehmer beauftragt einen Unterauftragnehmer für eine wichtige oder kritische Funktion unterstützende Dienstleistung, für welche vertraglich ein Verbot der Unterauftragsvergabe vereinbart wurde.</p> <p>f) Der Auftragnehmer verstößt in nicht unerheblicher Weise gegen die Bedingungen der Unterauftragsvergabe.</p>	
	Art. 5 Abs. 1, 2, 3 und 4 RTS-E SUB	<p>Der Auftragnehmer verpflichtet sich dem Auftraggeber alle erforderlichen Informationen für eine Überwachung der gesamten Auftragskette zur Bewertung und Dokumentation beim Auftraggeber zur Verfügung zu stellen. Die entsprechenden Verpflichtungen hat der Auftragnehmer in Verträgen mit Unterauftragnehmern zu vereinbaren. Dies beinhaltet neben quantitativen und qualitativen Leistungsindikatoren und den Dienstleisterberichten gemäß Kapitel XX (Klausel zu Art. 30 Abs. 3 lit. b DORA) der von ihm beauftragten Unterauftragnehmer für den vergebenen Auftrag auch die Vorlage der relevanten vertraglichen Vereinbarungen zwischen dem Auftragnehmer und Unterauftragnehmern sowie zwischen weiteren Unterauftragnehmern sofern sie die konkrete Dienstleistung betreffen. Insbesondere betrifft dies alle Informationen, welche bezüglich der Auftragskette in das Informationsregister gemäß Art. 28 Absatz 3 der VO (EU) 2022/2554, konkretisiert durch die VO (RTS-E SUB und ITS Register) einzutragen sind oder die für eine Beurteilung der Auswirkungen der Komplexität oder Länge der Kette auf die Fähigkeit effektiver</p>	Hinweis: Dafür kann der Auftraggeber dem Auftragnehmer einen auszufüllenden Fragebogen zur Verfügung stellen.

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		Überwachung durch den Auftraggeber oder die zuständigen Aufsichtsbehörden erforderlich sind. Zu diesem Zweck sind die Informationen aktuell zu halten.	
	Art. 4 Abs. 1 lit. j; 6 Abs. 1 und 2 RTS-E SUB	Sofern der Auftragnehmer wesentliche Änderungen an Unterauftragsverhältnissen beabsichtigt, einschließlich der erstmaligen oder weiteren Neubeauftragung von Unterauftragnehmern, hat dieser den Auftraggeber XX Wochen vorab zu informieren. Der Auftraggeber wird die Auswirkungen der geplanten Änderungen auf die Risikoanalyse bewerten und den Auftragnehmer über das Ergebnis informieren.	
	Art. 6 Abs. 2 RTS-E SUB	Der Auftragnehmer darf die Änderungen erst und nur dann durchführen, wenn der Auftraggeber bis zum Ablauf von XX Wochen nach Mitteilung der geplanten Änderung die Änderungen gebilligt oder diesen nicht widersprochen hat. Sofern für eine abschließende Risikobeurteilung weitergehende Informationen benötigt werden wird der Fristablauf für den Zeitraum bis zur Bereitstellung der Informationen gehemmt. Im Anschluss daran müssen dem Auftraggeber noch mindestens XX Wochen zur Bewertung der nachgelieferten Informationen verbleiben.	Im Zusammenspiel mit voriger Musterklausel.
	Art. 6 Abs. 3 RTS-E SUB	Der Auftraggeber hat das Recht Modifizierungen an der geplanten Änderung der Unterauftragsvergabe vor deren Umsetzung zu verlangen, wenn die Risikoanalyse ergibt, dass die geplante Änderung die Risikobereitschaft des Auftraggebers überschreitet. Er wird den Auftragnehmer über das Ergebnis der Risikoanalyse informieren. Finden Auftraggeber und Auftragnehmer in diesem Fall keine einvernehmliche Lösung, steht dem Auftraggeber ein Sonderkündigungsrecht zu.	

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

	<p>Art. 3 Abs. 1 lit. c RTS-E SUB</p>	<p>Der Auftragnehmer verpflichtet sich die mit dem Auftraggeber in diesem Vertrag geschlossenen wesentlichen vertraglichen Regelungen in den Verträgen mit Unterauftragnehmern derart nachzubilden, dass der Auftraggeber jederzeit in der Lage ist, seine rechtlichen und aufsichtsrechtlichen Verpflichtungen, insbesondere aus der Verordnung (EU) 2022/2554 folgend, fortlaufend einzuhalten. Er gewährt dem Auftraggeber, dessen Aufsichts- und Abwicklungsbehörde sowie von diesen benannten Dritten die gleichen vertraglichen Audit-, Zugangs- und Inspektionsrechte entlang der Kette von Unterauftragnehmern, welche IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen erbringen, wie sie der Auftragnehmer im Verhältnis zum Auftraggeber gewährt. [ggf. individuell zu ergänzen, etwa: Neben dem entsprechenden Niveau der Cybersicherheit betrifft dies insbesondere die Prüf-, Mitwirkungs- und Informationspflichten des Auftraggebers bzw. gegenüber dem Auftraggeber etc.].</p>	<p>Hinweis: im Einzelfall kann eine weitere Einschränkung möglich sein.</p>
<p>Elemente der (vorgelagerten) Due Diligence, welche optional auch vertraglich geregelt werden könnten</p>			
	<p>Art. 3 Abs. 1 lit. a, d RTS-E SUB</p>	<p>[optional] Der Auftragnehmer hat dem Auftraggeber gegenüber die Einzelheiten des Auswahlprozesses für Unterauftragnehmer sowie der Beteiligung an operativen Berichts- und Testpflichten offenzulegen und zu erläutern.</p>	
	<p>Art. 3 Abs. 1 lit. f RTS-E SUB</p>	<p>[optional] Der Auftragnehmer unterstützt den Auftraggeber bei der Analyse der Auswirkungen eines potentiellen Ausfalls des Unterauftragnehmers auf die digitale operationale Resilienz und finanzielle Robustheit des Auftraggebers. Hierzu wird er die</p>	

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		erforderlichen Informationen, gegenüber dem Auftraggeber offenlegen.	
	Art. 3 Abs. 2 RTS-E SUB	[optional] Der Auftraggeber wird die Risikoanalyse zum Einsatz von Unterauftragnehmern regelmäßig auf Veränderungen überprüfen, insbesondere hinsichtlich der unterstützten Funktion, IKT-Bedrohungen, Konzentrationsrisiken und geopolitischen Risiken. Der Auftragnehmer verpflichtet sich dem Auftraggeber die hierzu erforderlichen Informationen zur Verfügung zu stellen.	
Detailliertere Formulierung der Eingangsklausel unter teilweiser Einbeziehung weiterer Musterbausteine			
		<p>[Alt. 1: Zustimmungsregelung für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen]:</p> <p>Der Auftragnehmer darf die übernommene Tätigkeit nur dann ganz oder teilweise unterbeauftragen (Fremdbezug oder Unterauslagerung), wenn der Auftraggeber dieser Subdelegation schriftlich (Textform ist ausreichend) zugestimmt hat. Der Auftragnehmer hat dem Auftraggeber [ggf. mindestens XX Wochen - der Zeitraum ist individuell festzulegen] zuvor schriftlich (Textform ausreichend) unter Darlegung der Eignung und Zuverlässigkeit des Dritten sowie genauer Beschreibung der unterbeauftragten Tätigkeiten die geplante Subdelegation anzuzeigen. Der Auftragnehmer liefert sämtliche für eine Risikoanalyse beim Auftraggeber erforderliche Informationen. Dafür kann der Auftraggeber dem Auftragnehmer einen auszufüllenden Fragebogen zur Verfügung stellen.</p> <p>Der Auftraggeber hat das Recht, Änderungen an den vorgeschlagenen Änderungen der Untervergabe vor</p>	<p>Hinweis: Die detailliertere Formulierung "Zustimmungsvariante" enthält bereits Elemente aus:</p> <ul style="list-style-type: none"> • Art. 30 Abs. 2 lit. a DORA • Art. 5 Abs. 1 RTS-E SUB • Art. 5 Abs. 2 RTS-E SUB • Art. 6 Abs. 4 RTS-E SUB • Art 4 lit. h RTS-E SUB • Art. 4 lit I RTS-E SUB • Art. 4 lit c RTS-E SUB • Art. 4 lit. g RTS-E SUB • Art. 3 lit. f RTS-E SUB

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>deren Durchführung zu verlangen, wenn die Risikoanalyse ergibt, dass die geplante Untervergabe oder Änderungen der Untervergabe durch den Auftragnehmer den Auftraggeber Risiken im Sinne von Artikel 3 Absatz 1 RTS-E SUB aussetzt, die seine Risikobereitschaft übersteigen.</p> <p>Wenn der Auftraggeber seine schriftliche Zustimmung (Textform ist ausreichend) erteilt, verpflichtet sich der Auftragnehmer sicherzustellen, dass die übernommene Tätigkeit nach gleichen Standards und in gleicher Qualität wie nach diesem Vertrag erbracht wird. Insoweit werden der Auftragnehmer und der Unterauftragnehmer ebenfalls eine schriftliche Vereinbarung (Textform ist ausreichend) schließen. Hierin wird insbesondere sichergestellt, dass der Unterauftragnehmer vertraglich in dem erforderlichen Umfang die Pflichten des Auftragnehmers zu erfüllen hat und dass der Auftraggeber, dessen Innenrevision, Compliance-Beauftragte, Datenschutzbeauftragte, zentrales Auslagerungsmanagement, eine zuständige Aufsichtsbehörde sowie von diesen benannte Dritte (z.B. Wirtschaftsprüfer) ihre nach diesem Vertrag eingeräumten Rechte unmittelbar geltend machen können. Der Auftragnehmer bleibt im Falle einer Unterbeauftragung weiterhin gegenüber dem Auftraggeber berichtspflichtig. Der Auftragnehmer bleibt für die Erfüllung der unterbeauftragten Tätigkeiten verantwortlich als würden diese durch den Auftragnehmer selbst ausgeführt. Der Auftragnehmer legt dem Auftraggeber auf dessen Anforderung hin den Vertrag mit dem Unterauftragnehmer offen.</p> <p>[Optional] Der Auftraggeber ist rechtzeitig vor Vollzug einer schriftlich genehmigten Unterbeauftragung von</p>	
--	--	--	--

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>Dritten zu informieren. Der Auftraggeber hat auch nach schriftlich erteilter Zustimmung jederzeit das Recht, diese aus wichtigen Gründen zu widerrufen. Als wichtiger Grund gilt insbesondere, wenn</p> <ul style="list-style-type: none"> a) begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung ordnungsgemäß erbringt, b) die Geltendmachung der vorgenannten Rechte nicht sichergestellt ist, c) die zuständige Aufsichtsbehörde der Unterbeauftragung widerspricht, d) der Unterauftragnehmer seinen Sitz außerhalb der [EU/EWR] oder kundenbezogene Datenverarbeitung außerhalb der [EU/EWR] verlegt, e) durch die Unterbeauftragung einer Tätigkeit die Wirksamkeit der Beaufsichtigung dieser Tätigkeit durch den Auftraggeber in irgendeiner Weise beeinträchtigt wird, f) der Unterauftragnehmer nicht über ausreichende Ressourcen, Kenntnisse und Erfahrung für die Ausführung der jeweiligen Aufgaben verfügt oder g) die zuständige Aufsichtsbehörde daran gehindert wird zu kontrollieren, dass der Auftraggeber seine gesetzlichen Verpflichtungen einhält. 	
		<p>[Alt. 2 Widerspruchsregelung]:</p> <p>Der Auftragnehmer ist nur dann berechtigt, die übernommene Tätigkeit durch schriftlichen Vertrag (Textform ist ausreichend) ganz oder teilweise unterzubeauftragen (Fremdbezug oder</p>	<p>Hinweis: Die detailliertere Formulierung "Widerspruchsvariante" enthält bereits Elemente aus:</p>

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>Unterauslagerung), wenn sichergestellt ist, dass die übernommene Tätigkeit nach gleichen Standards und in gleicher Qualität wie nach diesem Vertrag erbracht wird. Dies setzt insbesondere voraus, dass der Unterauftragnehmer vertraglich in dem erforderlichen Umfang die Pflichten des Auftragnehmers zu erfüllen hat, und dass der Auftraggeber, dessen Innenrevision, Compliance-Beauftragte, Datenschutzbeauftragte, zentrales Auslagerungsmanagement, oder eine zuständige Aufsichtsbehörde sowie von diesen benannte Dritte (z.B. Wirtschaftsprüfer) ihre nach diesem Vertrag eingeräumten Rechte unmittelbar geltend machen können. Der Auftragnehmer bleibt im Falle einer Unterbeauftragung weiterhin gegenüber dem Auftraggeber berichtspflichtig. Der Auftragnehmer bleibt für die Erfüllung der unterbeauftragten Tätigkeiten verantwortlich als würden diese durch den Auftragnehmer selbst ausgeführt. Der Auftragnehmer legt dem Auftraggeber auf dessen Anforderung hin den Vertrag mit dem Unterauftragnehmer offen. Der Auftraggeber hat das Recht, Änderungen an den vorgeschlagenen Änderungen der Untervergabe vor deren Durchführung zu verlangen, wenn die Risikoanalyse ergibt, dass die geplante Untervergabe oder Änderungen der Untervergabe durch den Auftragnehmer den Auftraggeber Risiken im Sinne von Artikel 3 Absatz 1 RTS-E SUB aussetzt, die seine Risikobereitschaft übersteigen.</p> <p>Der Auftraggeber ist mit einer Frist von [ggf. mindestens XX Wochen - der Zeitraum ist je nach Unternehmen individuell festzulegen] vor dem Vollzug einer Unterbeauftragung schriftlich unter Darlegung der Eignung und Zuverlässigkeit des Dritten sowie genauer Beschreibung der</p>	<ul style="list-style-type: none"> • Art. 30 Abs. 2 lit. a DORA • Art. 5 Abs. 1 RTS-E SUB • Art. 5 Abs. 2 RTS-E SUB • Art. 6 Abs. 4 RTS-E SUB • Art 4 lit. h RTS-E SUB • Art. 4 lit I RTS-E SUB • Art. 4 lit c RTS-E SUB • Art. 4 lit. g RTS-E SUB • Art. 3 lit. f RTS-E SUB
--	--	--	---

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>unterzubeauftragenden Tätigkeiten zu informieren. Der Auftragnehmer liefert auf Anforderung weitere Informationen, die der Auftraggeber zur Risikoanalyse benötigt. Dafür kann der Auftraggeber dem Auftragnehmer einen auszufüllenden Fragebogen zur Verfügung stellen.</p> <p>Der Auftraggeber hat das Recht, der Unterbeauftragung aus wichtigen Gründen zu widersprechen. Als wichtiger Grund gilt insbesondere, wenn</p> <ol style="list-style-type: none"> a) begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung ordnungsgemäß erbringt, b) die Geltendmachung der vorgenannten Rechte nicht sichergestellt ist, c) die zuständige Aufsichtsbehörde der Unterbeauftragung widerspricht, d) der Unterauftragnehmer seinen Sitz außerhalb der [EU/EWR] oder kundenbezogene Datenverarbeitung außerhalb der [EU/EWR] hat, e) durch die Unterbeauftragung einer Tätigkeit die Wirksamkeit der Beaufsichtigung dieser Tätigkeit durch den Auftraggeber in irgendeiner Weise beeinträchtigt wird, f) der Unterauftragnehmer nicht über ausreichende Ressourcen, Kenntnisse und Erfahrung für die Ausführung der jeweiligen Aufgaben verfügt oder g) die zuständige Aufsichtsbehörde daran gehindert wird zu kontrollieren, dass der Auftraggeber seine gesetzlichen Verpflichtungen einhält. 	
--	--	--	--

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.

		<p>[Alt. 3, falls bereits Unterauftragnehmer bei Vertragsabschluss bewertet wurden und akzeptiert werden sollen]:</p> <p>Dem Auftraggeber ist bekannt, dass der Auftragnehmer derzeit bereits [Name/Anschrift des/der Unterauftragnehmer und ausgeübte Tätigkeit - oder Verweis auf eine entsprechende Vertragsanlage] in vorgenanntem Sinne eingeschaltet hat. [Optional bei Zustimmungsvariante]: Diese gelten als genehmigt.</p>	
--	--	---	--

* optionale bzw. ggf. unternehmensindividuell zu ergänzende Inhalte sind durch Klammerzusätze und gelbe Hinterlegung markiert.