HSW | RECHTSANWÄLTE HARDER SEDLMEIER WEITZEL

Mandanteninformation

Verträge mit IKT-Dienstleistern DORA-konform machen

In der öffentlichen Wahrnehmung wird die Daten-/Digitalisierungs-Regulierung von Diskussionen über AI Act, Data Act oder DSGVO geprägt. Dadurch geraten die anspruchsvollen Anforderungen der EU-Verordnung DORA in den Hintergrund.

Unbemerkt von vielen muss die gesamte Wertschöpfungskette in der Finanzbranche alle Verträge mit IKT-Dienstleistern anpassen oder komplett neuverhandeln. DORA enthält eine Fülle von Anforderungen, die spätestens ab dem 17.1.2025 in den Verträgen verbindlich enthalten sein muss.

Kluge IKT-Dienstleister leisten diese Vorbereitung schon jetzt, um auf Anfrage DORA-konforme Verträge anbieten können – inklusive bereits kalkulierter Mehrkosten.

Was ist in den Verträgen zu ändern?

Die von DORA direkt Betroffenen (vor allem Banken, Finanzunternehmen und Versicherungen) fragen nun ihre Juristen: Was müssen wir denn genau in die Verträge schreiben? Dieselbe Frage stellt sich im Umkehrschluss den IKT-Dienstleistern: Auf welche Klauseln müssen wir uns vorbereiten?

Praxistipp:	*Was anzupassen ist, steht im Gesetz. Über die meisten Klauseln lässt sich nicht streiten. Sie müssen nur an den richtigen Stellen im Vertrag oder den Leistungsbeschreibungen eingefügt werden.*

Ein häufiger Fehler ist dabei, nur in Kapitel V DORA zu schauen, weil das mit „Management des IKT-Drittparteienrisikos“ überschrieben ist. Indes ergeben sich Anpassungspflichten auch aus Vorschriften in anderen Kapiteln. Eine weitere Quelle sind die Durchführungsverordnungen zu DORA und die Umsetzungshinweise der BaFIN.

Praxistipp:	*Beachten Sie wirklich alle Anpassungspflichten, die quer über die gesamte DORA verteilt und in verschiedenen Durchführungsvorschriften zu finden sind!*

Behördliche Vorgaben?

Weil viele Unternehmen immer noch auf Vorgaben durch die BaFIN warten, hat diese am 8.7.2024 eine Tabelle „Mindestvertragsinhalte DORA“ veröffentlicht: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Aufsichtsmitteilung/dl_2024_06_10_Mindestvertragsinhalte_DORA.html?nn=19659504

Die Hilfestellung durch jenes Dokument hält sich indes in Grenzen: Es umfasst 69 Einträge, weil viele Anforderungen sehr kleinteilig dargestellt werden. Im Vertrag kann das je nach Einzelfall auf 15 bis 22 Klauseln verteilt erfolgen.

Gravierender ist: Die BaFIN gibt keine Vorgaben, was genau im Vertrag zu schreiben ist, selbst wenn in manchen Fällen eine allgemeingültige Formulierung möglich wäre. Auch sind die in Art. 30 Abs. 2 lit. h) DORA erwähnten „*Erwartungen der zuständigen Behörden an Mindestkündigungsfristen*“ in diesem Papier nicht enthalten.

Deshalb diese im Darstellungs-Umfang vereinfachte und mit konkreten Formulierungsvorschlägen ergänzte Darstellung.

Abschlusspflicht?

Häufig wird die Frage gestellt, ob IKT-Dienstleister zur Vertragsanpassung verpflichtet sind. Klare Antwort: Nach dem Gesetz nein. Denn es gibt keine gesetzliche Pflicht, Verträge an gesetzliche Änderungen anzupassen. Also muss diejenige Partei, die einen Vertrag anpassen will, mit der anderen Verhandlungen aufnehmen. § 313 BGB sieht bei schwerwiegender Änderung vertragswesentlicher Umstände vor, dass die „Anpassung des Vertrags verlangt werden“ kann. Ist die Anpassung für den anderen Partner nicht zumutbar, kann jener vom Vertrag zurücktreten.

Praxistipp:	*Compliance ist ein schönes Modewort. Es zwingt jedoch keinen Dienstleister, bestehende Verträge an geänderte Vorschriften anzupassen.*

Etwas anderes gilt nur, wenn im bestehenden Vertrag eine „stets gesetzkonforme Leistung“ vereinbart ist. Oder wenn der IKT-Dienstleister sich verpflichtet hat, alle durch Gesetzesänderungen erforderliche Leistungsänderungen vorzunehmen.

Praxistipp:	*Überlegen Sie, ob eine solche Pflicht im Rahmen der für DORA anstehenden Neuverhandlung in Ihre Verträge aufgenommen werden soll!*

Selbst in einem solchen Vertrag gilt jedoch: Fordert eine Partei gänzlich neue Leistungen oder Pflichten, kann die Gegenseite dafür eine Anpassung der Vergütung verlangen.

Unterschiedliche Verhandlungspositionen

Bei der von DORA erzwungene Neuverhandlung haben die beiden Vertragspartner unterschiedliche Interessen: Der IKT-Dienstleister will alle Mehraufwände bezahlt haben. Der Einkäufer versucht, möglichst viele der Änderungen ohne Mehrkosten akzeptiert zu bekommen.

Was tun bei erfolgloser Verhandlung?

Es ist nicht auszuschließen, dass ein angefragter IKT-Dienstleister sich der notwendigen Anpassung verweigert oder unangemessen hohe Mehrkosten dafür fordert.

Praxistipp:	*Verweigert ein IKT-Dienstleister die Anpassung gleich ganz, stellt dies nach unserer Rechtsauffassung einen Wegfall der Geschäftsgrundlage dar. Der berechtigt zur vorzeitigen Beendigung des Vertrages.* *Details hierzu sind mit Rechtsabteilung bzw. Anwälten im Detail abzuklären!*

In der Regel wird es Auseinandersetzung über die Ausgestaltung bestimmter Klauseln oder die Höhe der Kostenbeteiligung geben.

Ob und wann in einem solchen Fall ein Recht zur vorzeitigen Beendigung des Vertrages besteht, lässt sich pauschal nicht sagen. In jenem Fall bedarf es unbedingt einer engen Abstimmung mit Rechtsabteilung oder externen Juristen!

Ihre Ansprechpartner für dieses Thema:

Rechtsanwalt Bernd H. Harder
Rechtsanwalt Dr. Christian Weitzel

Auf den Folgeseiten:
Tabelle mit Klauselvorschlägen

Anpassungen für alle Verträge mit IKT-Dienstleistern

Nr.	Vorgabe	Quelle	Klausel
1.	Unterstützung des Auftraggebers im Hinblick auf dessen Berichtspflichten nach DORA	*Art. 1 Abs. 1 lit. a) Ziffer (i) bis (ii) DORA*	Der Provider wird den Auftraggeber in Erfüllung dessen Pflichten aus Art. 1 Abs. 1 lit. a) Ziffer (i) bis (iii) DORA angemessen unterstützen. Dazu wird er dem Auftraggeber • die für dessen Risikomanagement im Bereich der vertragsgegenständlichen Leistungen erforderlichen Informationen übermitteln, • die für die Meldung schwerwiegender IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen im Bereich der vertragsgegenständlichen Leistungen an die zuständigen Behörden erforderlichen Informationen übermitteln.
		Art. 1 Abs. 1 lit. a) Ziffer (iii) DORA	*Zusätzlich für die in Artikel 2 Absatz 1 Buchstaben a bis d DORA aufgeführten Finanzunternehmen:* • die zur Meldung schwerwiegender zahlungsbezogener Betriebs- und Sicherheitsvorfälle im Bereich der vertragsgegenständlichen Leistungen an die zuständigen Behörden erforderlichen Informationen übermitteln.

Nr.	Vorgabe	Quelle	Klausel
2.	*Für IKT-Systeme und Daten mit minimaler Ausfallzeit:* Vereinbarung von Zeitvorgaben für Wiederherstellungszeit und Wiederherstellungspunkte jeder Funktion zur Sicherstellung der vereinbarten Dienstleistungsgüte in Extremszenarien	*Art. 12 Abs. 6 DORA*	*Je nach konkreten Anforderungen und vertraglicher Leistung, z.B.:* SLS: **Datensicherung des Application Servers** SLO 1: Inkrementelle Sicherung aller geänderten Programme und Daten 1 x pro Tag SLO 2: Volle Sicherung aller Programme und Daten 1 x pro Woche SLS: **Leseprobe der eingesetzten Bänder zur Sicherstellung der vollständigen Rücksicherung** SLO 1 x pro ___ und Band SLS: **Zeitraum, zu dem eine vollständige Rücksicherung möglich ist** SLO: __ Tage/Jahre SLS: **Zeit zur Wiederherstellung einer Anwendung nach einem Stillstand** (Recovery Time Objective – RTO) SLO: __ h SLS: **Durchschnittliche Zeit bis zur Behebung eines Ausfalls** (Mean Time To Repair – MTTR) SLO: ___ h SLS: **Aktualität der Daten nach Wiederhestellung** (Recovery Point Objective – RPO) SLO: ___ h

Nr.	Vorgabe	Quelle	Klausel
3.	Ausreichend Zugangs-, Inspektions- und Auditrechte entsprechend dem Auditplan	*Art. 28 Abs. 6 DORA*	*Je nach Vorgaben aus vorab erstelltem Audit- und Inspektionsplan.* *Falls keine Zeiten vorgegeben werden sollen, dann z.B.:* Der Provider wird dem Auftraggeber (einschließlich dessen Interner Revision, Datenschutzbeauftragten und Compliance-Beauftragten), den aufgrund gesetzlicher Vorschriften bei dem Auftraggeber tätigen Prüfern, den Aufsichtsbehörden sowie den von den Aufsichtsbehörden mit der Prüfung beauftragten Stellen zu jeder Zeit die vollumfängliche und ungehinderte Einsicht und Prüfung des auf den Provider ausgelagerten Bereichs ermöglichen. Der Zugang zu rein kommerziellen Informationen oder zu Daten anderer Kunden des Providers ist dabei auszuschließen. Soweit eine Prüfung ergibt, dass die Leistungen oder das Verhalten des Providers nicht mit den vertraglichen oder gesetzlichen Anforderungen in Einklang stehen, werden die Parteien diese Tatsache erörtern. Sodann ist der Provider verpflichtet, unverzüglich sämtliche Maßnahmen zu ergreifen, die erforderlich oder zweckmäßig sind, um die betreffende Anforderungen zu erfüllen. Hat der Provider den Anlass für diese Maßnahmen nicht zu verantworten, werden die Kosten und Maßnahmen im Rahmen des Änderungsverfahrens vereinbart.
4.	Sicherstellung von Sonderkündigungsrechten gemäß Art. 28 Abs. 7 DORA	*Art. 28 Abs. 7 DORA*	Der Auftraggeber kann den betroffenen Leistungsschein oder den gesamten (Rahmen-) Vertrag insbesondere fristlos kündigen mit oder ohne in sein Belieben gestellter Auslauffrist, wenn: • ein erheblicher Verstoß des Providers gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen vorliegt; • Umstände vorliegen, die der Auftraggeber bei Überwachung seines IKT-Drittparteienrisikos feststellt und als geeignet einschätzt, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des Providers auswirken; • nachweisliche Schwächen des Providers in Bezug auf sein allgemeines IKT-Risikomanagement vorliegen 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; • die zuständige Behörde den Auftraggeber infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen kann.

Nr.	Vorgabe	Quelle	Klausel
5.	*Form:* Dokument in Papierform oder anderen, herunterladbarem und dauerhaft Schriftliches, dauerhaft zugänglichem Format *Änderungen* des Vertrages in Schriftform mit Datum und Unterschrift	*Art. 30 Abs. 1 DORA* *Art. 8 Abs. 4 RTS TPPol*	*Zum Beispiel mit Ausschluss der Textform:* Mündliche Nebenabreden oder Vorvereinbarungen bestehen nicht. Änderungen oder Ergänzungen dieses Vertrages bedürfen der Schriftform und sind mit dem Datum ihrer Ausfertigung zu versehen. Die Schriftform ist durch die Übersendung von e-Mails oder Textform nicht gewahrt, es sei denn, diese sind mit einer qualifizierten elektronischen Signatur (§ 126a BGB) versehen.
6.	Eindeutige, schriftliche Zuweisung von Rechten und Pflichten in jedem Vertrag mit IKT-Drittdienstleistern (= vollständige, detaillierte Leistungsbeschreibung)	*Art. 30 Abs. 1 und 2 lit. a) DORA*	*Keine Muster möglich*, weil abhängig von der eingekauften Leistung. Fest steht jedoch: Allgemeine Plattitüden wie „erbringt alle Dienstleistungen, die dafür notwendig sind", sind nicht mehr zulässig!
7.	Genaue Vereinbarung zu Standorten (Regionen/Länder), an denen IKT-Dienstleistungen bereitzustellen sind, Daten verarbeitet oder gespeichert werden sowie Pflicht zur Vorabnachricht bei Änderung dieser Standorte	*Art. 30 Abs. 2 lit. b) DORA*	*Keine allgemeingültigen Muster möglich, je nach Einzelfall anzupassen, z.B.:* Die vorgenannten Leistungen erbringt der Provider in seinem Rechenzentrum/-zentren in [Stadt]. Das zur Sicherstellung der Redundanz und für den K-Fall errichtete Ausweichrechenzentrum befindet sich in [Stadt]. Die Verlagerung eines Rechenzentrums muss vorab angezeigt werden und erfolgt kostenneutral für den Auftraggeber, außerhalb Deutschlands bedarf es der Zustimmung durch den Auftraggeber. Die Zustimmung hängt davon ab, ob die Einhaltung der erforderlichen datenschutzrechtlichen Anforderungen im Zielland sichergestellt ist. Sämtliche Verarbeitungsvorgänge der ausgelagerten Daten inklusive des Fernzugriffs dürfen ausschließlich in bzw. aus Deutschland erfolgen.
8.	Genaue Vereinbarung zu Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf Datenschutz und Datensicherheit (*Vorsicht:* weitergehend als DSGVO-Anforderungen!)	*Art. 30 Abs. 2 lit. c) DORA*	*Regelmäßig in Auftragsverarbeitungsvereinbarung enthalten, daher dort auf ausreichenden Schutzumfang und vollständige Umsetzung der DORA-Vorgaben prüfen!*

9.	Genaue Vereinbarung zur Sicherstellung des Zugangs zu Daten bei Insolvenz, Abwicklung oder Ausfällen des IKT-Drittdienstleisters	*Art. 30 Abs. 2 lit. d) DORA*	*In aller Regel im Rahmen eines gesonderten Leistungsscheins **Exit-Support*** *Bei **Insolvenz** hilft jedoch keine Regelung zu Exit-Leistungen, das erfordert meist **Escrow-Vereinbarungen**. Dies ist bei **SaaS-Verträgen** besonders wichtig. Inzwischen gibt es auch Escrow-Dienstleister, die eine Kopie der jeweiligen VM bereithalten und bei Ausfall des SaaS-Anbieters bereitstellen.* *Beispiel für eine sehr reduzierte **Exit-Support-Klausel** im Vertrag bei kleineren Auslagerungen:* Nach Ende der Laufzeit eines Leistungsscheins stellt der Provider dem Auftraggeber alle im Rahmen des Leistungsschein erstellten Unterlagen sowie die zu diesem Zeitpunkt im Provider-Rechenzentrum gespeicherten Daten auf maschinell lesbaren Datenträgern zur Verfügung, um eine einfache Übertragung und Fortführung der Datenverarbeitung zu ermöglichen. Das Datenformat, die Konfiguration der Datenträger und Preise werden im jeweiligen Leistungsschein vereinbart. Ein Zurückbehaltungsrecht an den Unterlagen oder Daten steht dem Provider nicht zu. Nach Eingang der schriftlichen Mitteilung, dass Auftraggeber alle übergebenen Daten hat lesen und verarbeiten können, wird der Provider diese auf allen seinen Systemen und Datenträgern unverzüglich löschen und die Löschung schriftlich bestätigen. Der Provider ist verpflichtet, den Auftraggeber im Falle einer vollständigen oder teilweisen Beendigung dieses Vertrages bei der Überleitung der betroffenen Leistungen auf einen Folgeanbieter zu unterstützen. „Folgeanbieter" ist entweder der Auftraggeber selbst oder ein von ihm beauftragter Dritter. Die Unterstützung umfasst alle Leistungen, die für eine ordnungsgemäße Überleitung der vertraglichen Leistungen auf den Folgeanbieter erforderlich oder zweckdienlich sind. Zeitlich sind dabei durch den Provider, soweit dies zumutbar ist, die Vorgaben des Auftraggebers einzuhalten. Im Rahmen der Exit-Unterstützung leistet der Provider insbesondere Folgendes: • Angemessene und zeitnahe Unterstützung des Auftraggebers bei der Erstellung und Durchführung von Ausschreibungen für die betroffenen Leistungen, einschließlich der Information über die bislang durch den Provider für die Erbringung der Leistungen eingesetzten Ressourcen; • Zusammenarbeit mit dem Folgeanbieter zum Zwecke einer ordnungsgemäßen Überleitung der betroffenen Leistungen, einschließlich der Ausarbeitung und Umsetzung eines detaillierten Überleitungsplans;

Nr.	Vorgabe	Quelle	Klausel
			• Schulung, Einweisung oder sonstige Vermittlung von Kenntnissen, die der Folgeanbieter für die ordnungsgemäße Erbringung der betroffenen Leistungen benötigt, einschließlich der Information über die eingesetzten Systeme, Abläufe und Prozesse; • Herausgabe aller Daten, Informationen und Unterlagen, die dem Auftraggeber nach diesem Vertrag zustehen, sowie Übergabe aller sonstigen im Besitz des Provider befindlichen Daten, Informationen und Unterlagen, die erforderlich sind, um dem Folgeanbieter die eigenverantwortliche Durchführung der Leistungen zu ermöglichen, und zwar jeweils in einer durch den Folgeanbieter ohne weiteres verwendbaren Form. • Der Auftraggeber ist ungeachtet der vertraglichen Vertraulichkeitspflicht berechtigt, Informationen, die das vorliegende Vertragsverhältnis betreffen, gegenüber möglichen Folgeanbietern offen zu legen, soweit dies für eine ordnungsgemäße Überleitung der Leistungen nach diesem Vertrag erforderlich oder zweckdienlich ist, einschließlich der vorliegenden Vertragsdokumentation (ausgenommen die Vergütungsinformationen). Den Folgeanbietern ist insoweit eine Vertraulichkeitsverpflichtung aufzuerlegen. Die Exit-Unterstützung ist unabhängig davon zu erbringen, aus welchem Grund dieser Vertrag – ganz oder teilweise – beendet wird, d. h. auch im Falle einer Kündigung aus wichtigem Grund durch eine der Parteien oder einer Ausübung des Sonderkündigungsrechts durch den Auftraggeber. Der Auftraggeber ist berechtigt, den Zeitpunkt der Beendigung der Leistungserbringung durch den Provider hinsichtlich der Gesamtheit oder eines Teils der betroffenen Leistungen einmalig oder mehrmalig zu verschieben, wobei der Beendigungszeitpunkt insgesamt höchstens um zwölf Monate ab dem ursprünglich vorgesehenen Beendigungszeitpunkt verschoben werden darf. Während eines solchen Verlängerungszeitraums gelten die Bestimmungen dieses Vertrages unverändert fort. Der Auftraggeber wird den Provider 90 Tage im Voraus schriftlich über die jeweilige Verschiebung informieren. Für die Erbringung der in dieser Klausel beschriebenen Exit-Unterstützung schuldet der Auftraggeber Provider [keine gesonderte Vergütung] / [Vergütung spezifizieren]. Der Provider verpflichtet sich, auch nach Abschluss der Überleitung der betroffenen Leistungen auf den Folgeanbieter noch für die Dauer von bis zu zwölf Monaten für die Erbringung von Teilbereichen solcher Leistungen zur Beantwortung von Fragen und zur Erbringung von Beratungsleistungen zur Verfügung zu stehen. Provider kann hierfür eine angemessene Vergütung gemäß Anlage: Preisübersicht verlangen.

<table>
<tr><th>Nr.</th><th>Vorgabe</th><th>Quelle</th><th>Klausel</th></tr>
<tr><td>10.</td><td>Vereinbarung zur Dienstleistungs-güte (= SLA) einschließlich Aktualisierung und Überarbeitung</td><td>Art. 30 Abs. 1 und 2 lit. e) DORA</td><td>Erfordert Leistungsschein mit genauer Festlegung von Service Levels.
Beispiel für einleitende Klausel zur Erläuterung:
Alle qualitativen und quantitativen Anforderungen an die hierzu erforderlichen Leistungen sind im Folgenden aufgeführt. Zu jeder Leistung ist die Mindestgüte beschrieben und anhand von Messgrößen prüfbar gemacht („Service Level“).
Die Beschreibung eines jeden Service Levels sieht wie folgt aus:
<table>
<tr><th>Nr.</th><th>Service Item</th><th>SLS</th><th>SLO</th><th>Messpunkt</th></tr>
<tr><td rowspan="2">Referenz-Nummer</td><td>Worauf bezieht sich der Service Level?</td><td>Service Level Specification:
Beschreibung der geschuldeten Dienstleistung</td><td>Service Level Objective:
▪ Messbare Parameter der Leistungserfüllung als Zielwert
▪ Meist Erreichbarkeit, sonstige Zeitfaktoren (z.B. Wiederanlauf), Zuverlässigkeit oder Qualität</td><td>Wer misst wo und wie?</td></tr>
<tr><td colspan="3">Verstoß
Beschreibung des Verstoßes</td><td>Service Credits
Anzahl</td></tr>
</table>
</td></tr>
<tr><td>11.</td><td>Vereinbarung zu Unterstützungs-leistungen bei IKT-Vorfällen bei vertragsrelevanten Dienstleistungen</td><td>Art. 30 Abs. 2 lit. f) DORA</td><td>Keine allgemeingültigen Muster möglich, je nach Einzelfall anzupassen, z.B.:
Tritt bei dem Auftraggeber ein IKT-Vorfall im Zusammenhang mit einer vertragsgegen-ständlichen Leistung ein, wird der Provider unverzüglich folgende Unterstützung erbringen:
[genau detaillieren]
[entweder:] Diese Unterstützung wird nicht gesondert vergütet. [oder:] Die Kosten für die erforderliche Unterstützung durch den Provider wird jenem nach Zeit und Aufwand gegen Tätigkeitsnachweis gemäß Anlage: Preisübersicht vergütet.</td></tr>
<tr><td>12.</td><td>Vereinbarung zu vollumfänglicher Zusammenarbeit mit zuständigen DORA-Behörden</td><td>Art. 30 Abs. 2 lit. g) DORA</td><td>Der Provider verpflichtet sich, auf Anforderung durch den Auftraggeber mit den für jenen zuständigen Aufsichts- oder Abwicklungs-Behörden vollumfänglich zusammenzuarbeiten.
Insbesondere wird der Provider jenen Behörden zu jeder Zeit
• Kontakt zu den von diesen benannten Personen ermöglichen und jene für die angeforderte Zusammenarbeit entsprechend autorisieren bzw. freistellen;
• die angeforderten Informationen und Dokumente zur Verfügung stellen;
• die vollumfängliche und ungehinderte Einsicht und Prüfung des auf den Provider ausgelagerten Bereichs ermöglichen.</td></tr>
</table>

Nr.	Vorgabe	Quelle	Klausel
13.	Kündigungsrechte und Mindest-kündigungsfristen gemäß Art. 30 Abs. 2 lit h) DORA	*Art. 30 Abs. 2 lit. h) DORA*	*Dürfte nach derzeitigem Erkenntnisstand mit den Sonderkündigungsrechten gemäß Art. 28 Abs. 7 DORA zusammenfallen.* *Erwartungen der zuständigen Behörden an Mindestkündigungsfristen sind noch nicht bekannt.*
14.	Vereinbarung von Bedingungen für Teilnahme an Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationellen Resilienz	*Art. 30 Abs. 2 lit. i) DORA*	*Keine allgemeingültigen Muster möglich, je nach Einzelfall anzupassen, z.B.:* Der Auftraggeber hält für seine Mitarbeiter und Dienstleister regelmäßig Maßnahmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationellen Resilienz ab. Der Provider wird an diesen Maßnahmen bis zu __ mal im Kalenderjahr mit bis zu __ Mitarbeitern teilnehmen. [Details zur Kostentragung]

Anpassungen für Verträge zur Unterstützung kritischer oder wichtiger Funktionen

Für Verträge zur Unterstützung kritischer oder wichtiger Funktionen schreibt DORA noch zusätzliche Anforderungen vor:

Nr.	Vorgabe	Quelle	Klausel
15.	Vereinbarung von Tests der IKT-Geschäftsfortführungspläne mit Providern, die kritische oder wichtige Funktionen übernehmen	*Art. 11 Abs. 4 DORA*	*In einem detaillierten Leistungsschein sollten Desaster Recovery-Pläne, -Maßnahmen und -Tests detailliert beschrieben sein.* *Keine allgemeingültigen Muster möglich, je nach Einzelfall anzupassen, z.B.:* Der Auftraggeber unterwirft seine IKT-Geschäftsfortführungspläne regelmäßigen Tests, an denen auch der Provider beteiligt wird. Dazu wird der Provider bis zu __ mal im Kalenderjahr [genaue Beschreibung]
16.	Vereinbarung von Exit-Support und Übergangszeiträumen gemäß Art. 28 Abs. 8 und 30 Abs. 3 lit. f) DORA	*Art. 28 Abs. 8 DORA* *Art. 30 Abs. 3 lit. f) DORA*	*In aller Regel im Rahmen eines gesonderten Leistungsscheins* ***Exit-Support*** *Beispiel für eine sehr reduzierte* ***Exit-Support-Klausel*** *im Vertrag bei kleineren Auslagerungen siehe oben.*

Nr.	Vorgabe	Quelle	Klausel
17.	Abwägung der Risiken einer zugelassenen Untervergabe mit entsprechenden Vorgaben an Hauptunternehmer	*Art. 29 Abs. 2, 30 Abs. 2 lit a) DORA* *Art. 4 RTS-E SUB* *Art. 6 Abs. 1-4 RTS-E SUB* *Art. 7 Abs. 1 lit. a) bis c) RTS-E SUB*	***Untervergabe*** *je nach konkreten Anforderungen und vertraglicher Leistung, allgemein gehalten z.B.:* Die Einschaltung von Subunternehmern und Vorlieferanten bedarf mit Ausnahme von Hard- oder Software-Lieferanten, die für die Leistungserbringung erforderlich sind, der vorherigen ausdrücklichen schriftlichen Zustimmung des Auftraggebers. Sie kann insbesondere dann verweigert werden, wenn Zweifel an der Qualifikation und/oder der finanziellen Leistungsfähigkeit des Subunternehmers/Vorlieferanten bestehen. *Untervergabe individuell vorgegeben:* Eine Untervergabe ist nur für die Leistungsbereiche [___] zulässig und bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Auftraggebers. Sie kann insbesondere dann verweigert werden, wenn Zweifel an der Qualifikation und/oder der finanziellen Leistungsfähigkeit des Subunternehmers/Verkäufers bestehen. ***Weitergabe Vertragsbedingungen*** *pauschal (vertragliche Wirksamkeit zweifelhaft):* In jedem Vertrag mit seinen Subunternehmern wird der Provider die vertraglichen Bedingungen aus diesem Vertrag durchreichen, die zur Aufrechterhaltung der gesetzlichen Vorgaben zur digitalen Resilienz erforderlich sind. Dies gilt insbesondere auf die in diesem Vertrag vereinbarten Inspektions- und Audit- sowie Kündigungsrechte des Auftraggebers *Besser:* Genau vorgeben, was an Subunternehmer durchgereicht werden muss ***Überwachungspflicht Provider:*** Der Provider wird die Leistungserbringung durch Subunternehmer kontinuierlich und effektiv überwachen um sicherzustellen, dass diese den vertraglichen Anforderungen insbesondere im Hinblick auf die gesetzlichen Anforderungen an digitale Resilienz entsprechen. Dabei wird er folgende Meldungspflichten gegenüber dem Auftraggeber erfüllen: [genau aufzählen, wozu umgehend Meldung gemacht werden muss] ***Mitteilung Änderungen:*** Der Provider wird jegliche substantielle Änderungen in Verträgen mit Subunternehmern über vertragsgegenständliche Leistungen mit ausreichend zeitlichen Vorlauf mit dem Auftraggeber abstimmen, damit jener die damit verbundenen Risiken einschätzen und etwaige Vorgaben zur Vertragsänderung machen kann. Die Vertragsänderung mit dem Subunternehmer darf erst nach Zustimmung des Auftraggebers vereinbart werden.

Nr.	Vorgabe	Quelle	Klausel
18.	Sonderkündigungsrechte in Bezug auf Unterauftragnehmer	*Art. 7 Abs. 1 RTS-E SUB*	Der Auftraggeber kann den betroffenen Leistungsschein oder den gesamten (Rahmen-) Vertrag insbesondere fristlos kündigen mit oder ohne in sein Belieben gestellter Auslauffrist, wenn der Provider: • ohne Einwilligung des Auftraggebers kritische oder wichtige Funktionen aus den vertragsgegenständlichen Leistungen untervergibt; oder • ohne Einwilligung des Auftraggebers substantielle Änderungen an den Verträgen zur Untervergabe vertragsgegenständlicher Leistungen vornimmt; oder • in seinen Verträgen mit den Subunternehmern die vertraglichen Bedingungen aus diesem Vertrag nicht im vereinbarten Umfang durchreicht; oder • die Pflicht zur vereinbarten Überwachung der Subunternehmer verletzt.
19.	SLA mit präzisen quantitativen und qualitativen Leistungszielen, wirksame Überwachung (Reporting!) und Korrekturmaßnahmen bei SLA-Verletzung	*Art. 30 Abs. 3 lit. a) DORA*	*Zu den Service Levels siehe bereits oben!* *Zum Reporting gibt es meist eigene Leistungsscheine oder detaillierte Abschnitte im SLA.* *Hier beispielhaft ein paar ausgewählte Klauseln dazu:* Der Provider stellt dem Auftraggeber Berichte zum dritten Werktag eines jeden Kalendermonats zur Verfügung, die eine Feststellung der erreichten Service Level beinhalten (Basisreporting). Das Basisreporting erfolgt nach diesem Schema: [Details] Über das Basisreporting hinaus stellt der Provider dem Auftraggeber auf schriftliches Verlangen die für ihn aufgezeichneten Systemdaten, die eine Überprüfung der vom Provider zur Verfügung gestellten Berichte ermöglichen, zur Verfügung. Die Kosten für die Ermittlung und Bereitstellung solcher über das Basisreporting hinausgehenden Systemdaten trägt der Provider, wenn die vertraglich vereinbarte Verfügbarkeit nicht erreicht wurde und die Daten dieses belegen. Anderenfalls hat der Auftraggeber die entsprechenden Kosten an den Provider zu erstatten. Dieses Verlangen kann nicht später als vier Wochen nach Überlassung des Basisreporting geltend gemacht werden.
20.	Kündigungsfristen, Melde- und Berichtspflichten zu Entwicklungen beim IKT-Drittdienstleister, die sich wesentlich auf dessen Fähigkeit zur Vertragserfüllung auswirken könnten	*Art. 30 Abs. 3 lit. b) DORA*	*Keine allgemeingültigen Muster möglich, je nach Einzelfall anzupassen.*

Nr.	Vorgabe	Quelle	Klausel
21.	Implementierung und Tests von Notfallplänen und ausreichend Sicherheitsmaßnahmen	*Art. 30 Abs. 3 lit. c) DORA*	*In einem detaillierten Leistungsschein sollten Desaster-Recovery-Pläne, -Maßnahmen und -Tests detailliert beschrieben sein.* *Keine allgemeingültigen Muster möglich, je nach Einzelfall anzupassen!*
22.	Pflicht zur Beteiligung und uneingeschränkten Mitwirkung an TLPTs	*Art. 30 Abs. 3 lit. d) DORA*	*Keine allgemeingültigen Muster möglich, je nach Einzelfall anzupassen, z.B.:* Mindestens alle drei Jahre hat der Auftraggeber bedrohungsorientierte Penetrationstests (Threat-Led Penetration Testing – TLPT) nach den Vorgaben von Art. 26 und 27 DORA durchzuführen. Dabei sind die nach diesem Vertrag ausgelagerten Funktionen mit zu testen. Der Provider wird die vom Auftraggeber angeforderte Beteiligung und Unterstützung jener Tests im Rahmen der vertraglich ausgelagerten Funktionen uneingeschränkt unterstützen und dazu jede erforderliche und angemessene Unterstützung leisten. [Details zur Kostentragung]
		Art. 8 Abs. 2 lit. b) RTS TPPol	*Wo angemessen:* Pooled TLPTs mit anderen Auftraggebern mit demselben Vertragsinhalt

Nr.	Vorgabe	Quelle	Klausel
23.	Umfassende Audit- und Überwachungsrechte	*Art. 30 Abs. 3 lit. e) DORA* *Art. 8 Abs. 3 lit. g) RTS TPPol*	*Allgemeingültiger Teil:* Der Provider wird dem Auftraggeber (einschließlich dessen Interner Revision, Datenschutzbeauftragten und Compliance-Beauftragten), den aufgrund gesetzlicher Vorschriften bei dem Auftraggeber tätigen Prüfern, den Aufsichtsbehörden sowie den von den Aufsichtsbehörden mit der Prüfung beauftragten Stellen zu jeder Zeit die vollumfängliche und ungehinderte Einsicht und Prüfung des auf den Provider ausgelagerten Bereichs ermöglichen. Der Zugang zu rein kommerziellen Informationen oder zu Daten anderer Kunden des Providers ist dabei auszuschließen. Insbesondere wird der Provider dabei • Kontakt zu den von diesen benannten Personen ermöglichen und jene für die angeforderte Zusammenarbeit entsprechend autorisieren bzw. freistellen; • die angeforderten Informationen und Dokumente zur Verfügung stellen; • die Anfertigung von Scans oder Kopien von einschlägigen Unterlagen vor Ort ermöglichen, sofern diese für die Geschäftstätigkeit des Providers entscheidende Bedeutung zukommt; • die vollumfängliche und ungehinderte Einsicht und Prüfung des auf den Provider ausgelagerten Bereichs ermöglichen. Sollten bei solchen Prüfungen die Rechte anderer Kunden betroffen sein, hat der Provider Anspruch auf Vereinbarung eines alternativen Bestätigungsniveaus, das den gesetzlichen Anforderungen entspricht. Soweit für das Risikomanagement des Auftraggebers nachvollziehbar erforderlich und in angemessenen Abständen kann der Auftraggeber eine Ausdehnung des Prüf- und Audit-Pflichten auch auf andere Systeme und Überwachungseinrichtungen verlangen *Zusätzlich zu vereinbaren und je nach Einzelfall anzupassen* • Einzelheiten zu Umfang der Inspektionen • Einzelheiten zu Häufigkeit der Inspektionen • Einzelheiten zum Inspektionsverfahren *Abweichend davon bei Kleinstunternehmen zulässig:* Vereinbarung zur Übertragung der Zugangs- Inspektions- und Auditrechte auf vom Auftraggeber benannten unabhängigen Dritten, dem vorstehende Auskünfte und Rechte zu gewähren sind

Nr.	Vorgabe	Quelle	Klausel
		Art. 8 Abs. 2 lit. b) RTS TPPol	*Wo angemessen:* Pooled Audits mit anderen Auftraggebern mit demselben Vertragsinhalt
		Art. 8 Abs. 2 lit. c) RTS TPPol *Art. 8 Abs. 3 lit. h) RTS TPPOL*	*Wo angemessen:* Zertifizierungen durch Zertifizierungsinstitutionen Alle vorstehenden Prüfrechte bleiben von vorgelegten Zertifizierungen oder Prüfberichten interner Abteilungen bzw. externen Auditoren des Providers unberührt.
		Art. 8 Abs. 2 lit. d) RTS TPPol	*Wo angemessen:* Bereitstellung von Auditreports von internen Abteilungen bzw. externen Auditoren des Providers