Vertragsnachtrag

zum

vom
– nachfolgend „Hauptvertrag" –

zwischen

– nachfolgend „Kunde" –

und

GFOS GmbH
Am Lichtbogen 9
45141 Essen
– nachfolgend „GFOS" –

– Kunde und GFOS nachfolgend auch einzeln „Partei" oder gemeinsam „Parteien" genannt –

Mit Blick auf die geänderten regulatorischen Anforderungen durch das Inkrafttreten der DORA-VO (Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationelle Widerstandsfähigkeit des Finanzsektors) sowie den auf ihrer Grundlage erlassenen Durchführungsverordnungen vereinbaren die Parteien, dass die nachfolgende Anlage „Anlage zur Umsetzung regulatorischer Anforderungen nach DORA-VO" (DORA-VO-Anlage) Vertragsbestandteil des Hauptvertrages wird. Die Parteien nehmen hiermit Bezug auf die DORA-VO-Anlage und sind sich darüber einig, dass die dortigen Bestimmungen als Ergänzungen des Hauptvertrags gelten und – soweit die Bestimmungen der DORA-VO-Anlage bereits vertraglich geregelte Inhalte betreffen – diese Vertragsinhalte durch die betreffenden Bestimmungen der DORA-VO-Anlage entsprechend angepasst werden. Alle übrigen vertraglichen Vereinbarungen des Hauptvertrages gelten – soweit sie nicht durch die diesem Nachtrag beigefügte Anlage angepasst werden – unverändert fort. Die in der DORA-VO-Anlage enthaltenen Regelungen gelten bei Unklarheiten oder Widersprüchen zu den Regelungen des Hauptvertrages in ihrem jeweiligen spezifischen Anwendungsbereich vorrangig vor den Regelungen des Hauptvertrages.

[Kunde]	GFOS
_____	_____
Ort, Datum:	Ort, Datum:
_____	_____
Name(n) in Klarschrift	Name(n) in Klarschrift
_____	_____
Firmenstempel und Unterschrift(en)	Firmenstempel und Unterschrift(en)

Anlage zur Umsetzung regulatorischer Anforderungen nach DORA-VO (DORA-VO-Anlage)

Der Kunde und GFOS haben einen Vertrag zur Überlassung und Nutzung von GFOS-Softwareprodukten sowie zur Erbringung zugehöriger IT-Leistungen abgeschlossen.

Der Kunde hat GFOS bestätigt, dass die DORA-VO (Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationelle Widerstandsfähigkeit des Finanzsektors) auf den Kunden und die Nutzung bestimmter von GFOS im Rahmen des Vertrags bereitgestellter IKT-Dienstleistungen durch den Kunden Anwendung findet.

Um den Kunden bei der Erfüllung seiner Verpflichtungen gemäß DORA-VO in Bezug auf Drittanbieter von IKT-Dienstleistungen zu unterstützen, haben die Parteien vereinbart, die Bedingungen des bestehenden Vertrages um die Regelungen dieser DORA-VO-Anlage wie folgt zu ergänzen.

1. DEFINITIONEN UND AUSLEGUNG

1.1 In dieser Anlage haben die folgenden Begriffe haben die folgenden Bedeutungen:

1.1.1 Anlage bezeichnet diese DORA-VO-Anlage einschließlich ihrer Anhänge;

1.1.2 Dienstleistungen bezeichnet die von GFOS im Rahmen des Vertrags erbrachten Leistungen im Zusammenhang mit der Überlassung von GFOS-Softwareprodukten sowie der Erbringung zugehöriger IT-Leistungen;

1.1.3 DORA-VO bezeichnet die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011;

1.1.4 Hyperscaler bezeichnet ein Unternehmen mit nicht völlig unerheblicher Marktpräsenz, das in der Lage ist, seine Infrastruktur, insbesondere IT-Systeme, Server und Rechenzentren, in einem sehr großen Maßstab zu skalieren, um so selbst große Datenmengen zu verarbeiten;

1.1.5 IKT-Dienstleistungen hat die in Art. 3 Nr. 21 DORA-VO festgelegte Bedeutung;

1.1.6 IKT-Drittparteienrisiko hat die in Art. 3 Nr. 18 DORA-VO festgelegte Bedeutung;

1.1.7 IKT-bezogener Vorfall hat die in Art. 3 Nr. 8 DORA-VO festgelegte Bedeutung;

1.1.8 Kundendaten bezeichnet alle Daten (einschließlich personenbezogener Daten und nicht-personenbezogener Daten), die GFOS vom Kunden zur Verfügung gestellt und von GFOS im Rahmen der Erbringung der Dienstleistungen verarbeitet, insbesondere gespeichert, werden;

1.1.9 KWF bedeutet kritische oder wichtige Funktion.

1.1.10 KWF-relevante Dienstleistungen sind Dienstleistungen, welche vom Kunden in 0. ANHANG - Relevante Dienstleistungen als Dienstleistungen bestimmt wurden, die kritische oder wichtige Funktionen des Kunden unterstützen, und die dort in der Spalte mit der Überschrift "KWF" mit einem "J" gekennzeichnet sind;

1.1.11 Relevante Dienstleistungen bezeichnet die in 0. ANHANG - Relevante Dienstleistungen genannten Dienstleistungen, welche nach Auffassung der

Parteien IKT-Dienstleistungen im Sinne der DORA-VO sind;

1.1.12 Service-Level bezeichnet die im Vertrag festgelegten Service-Level;

1.1.13 TLPT (TLPT-Threat-Led Penetration Testing = bedrohungsorientierte Penetrationstests) hat die in Art. 3 Nr. 17 DORA-VO festgelegte Bedeutung;

1.1.14 Vertrag bezeichnet die Vereinbarung zwischen dem Kunden und GFOS über die Erbringung der jeweiligen Dienstleistungen.

1.1.15 Zuständige Behörden bezeichnet die jeweils zuständigen Behörden gemäß Art. 46 DORA-VO.

1.2 Alle weiteren Begriffe haben die in der DORA-VO festgelegte Bedeutung.

1.3 Die Anhänge dieser Anlage sind Bestandteil dieser Anlage.

2. ALLGEMEIN

2.1 Die Bestimmungen in dieser Anlage gelten nur wenn und soweit:

2.1.1 die DORA-VO für den Kunden gilt; und

2.1.2 es sich bei den Dienstleistungen um IKT-Dienstleistungen handelt, die in den Geltungsbereich der DORA-VO fallen und daher zu den Relevanten Dienstleistungen gehören; dementsprechend werden die Bestimmungen des Vertrages durch diese Anlage in Bezug auf andere vertragsgegenständliche Dienstleistungen, die keine Relevanten Dienstleistungen sind, nicht geändert.

2.2 Diese Anlage gibt dem Kunden nicht das Recht, von GFOS die Erbringung von zusätzlichen vergütungsfreien Leistungen zu fordern, die nicht bereits im Leistungsumfang des Vertrages enthalten sind.

2.3 GFOS und der Kunde sind sich darüber einig, dass die Bestimmungen dieser Anlage als Ergänzungen des Vertrags gelten und – soweit die Bestimmungen dieser Anlage bereits vertraglich geregelte Inhalte betreffen – diese Vertragsinhalte durch die betreffenden Bestimmungen der Anlage entsprechend angepasst werden. Alle übrigen vertraglichen Vereinbarungen des Vertrages gelten – soweit sie nicht durch diese Anlage angepasst werden – unverändert fort. Die in der Anlage enthaltenen Regelungen gelten bei Unklarheiten oder Widersprüchen zu den Regelungen des Vertrages in ihrem jeweiligen spezifischen Anwendungsbereich vorrangig vor den Regelungen des Vertrages.

2.4 Es liegt in der alleinigen Verantwortung des Kunden zu bestimmen, ob die in dieser Anlage vereinbarten Regelungen und Maßnahmen angemessen und ausreichend sind, um ihm die Einhaltung seiner gesetzlichen Verpflichtungen aus der DORA-VO zu ermöglichen.

3. DIENSTLEISTUNGEN

3.1 GFOS erbringt die Dienstleistungen gemäß der vertraglich vereinbarten Leistungs- bzw. Produktbeschreibung.[1]

3.2 GFOS wird die vertraglich vereinbarten Service-Level erfüllen.[2]

3.3 In 0. ANHANG - Standorte sind die Standorte aufgeführt, an denen zum Zeitpunkt der Vereinbarung dieser Anlage die Dienstleistungen bereitgestellt werden und an denen die

[1] Art. 30 Abs. 2 lit. a) DORA
[2] Art. 30 Abs. 2 lit. e) bzw. 30 Abs. 3 lit. a) DORA

Kundendaten verarbeitet werden, einschließlich des Speicherorts.[3] GFOS kann diese Standorte ändern, sofern GFOS dies mindestens dreißig (30) Tage im Voraus ankündigt.[4]

4. SICHERHEIT

4.1 Bei der Erbringung der Dienstleistungen setzt GFOS die im Vertrag vereinbarten Informationssicherheitsstandards[5] um und stellt sicher, dass diese Standards mindestens das gleiche Schutzniveau bieten, wie es durch die derzeitige Zertifizierung von GFOS nach ISO 27001:2022 nachgewiesen wird.

4.2 GFOS ergreift geeignete Maßnahmen, um:

4.2.1 zu gewährleisten, dass die Kundendaten für den Zugriff und die Nutzung durch den Kunden in Übereinstimmung mit den Vertragsbedingungen verfügbar sind;

4.2.2 die Echtheit der Kundendaten zu überprüfen, indem unter anderem gewährleistet wird, dass die Kundendaten nur von befugten Personen und Systemen verarbeitet, übermittelt oder abgerufen werden; und

4.2.3 die Authentizität und Vertraulichkeit der Kundendaten zu wahren, einschließlich des Schutzes vor unbefugtem Zugriff, Änderung, Löschung oder Verfälschung gemäß Ziffer 4.1 und den ggf. zusätzlich im Vertrag geregelten Bedingungen.

5. ZUGANG, WIEDERHERSTELLUNG UND RÜCKGABE VON DATEN[6]

5.1 Der Kunde hat das Recht, auf die Dienstleistungen zuzugreifen, um die in den Dienstleistungen gespeicherten Kundendaten in ein leicht zugängliches Format zu exportieren:

5.1.1 bei Beendigung des Vertrages; oder

5.1.2 bei Insolvenz, Abwicklung oder Einstellung der Geschäftstätigkeit von GFOS.

5.2 Das Recht nach Ziffer 5.1 gilt für einen Zeitraum von neunzig (90) Tagen nach Eintritt des in Ziffer 5.1.1 oder 5.1.2 genannten Ereignisses ("Ausstiegszeitraum"). Während des Ausstiegszeitraums gilt:

5.2.1 GFOS wird die Kundendaten nicht löschen;

5.2.2 Abgesehen von den Dienstleistungen gemäß Ziffer 5.1 oder Ziffer 5.3, schuldet GFOS keine weiteren Leistungen; und

5.2.3 Sofern die in Ziffer 5.1 oder Ziffer 5.3 genannten Dienstleistungen erbracht werden, findet der Vertrag auch für solche Dienstleistungen Anwendung.

5.3 Benötigt der Kunde während des Ausstiegszeitraums weitere Unterstützung von GFOS in Bezug auf den Zugang, die Wiederherstellung oder die Rückgabe von Kundendaten, wird GFOS den Kunden im angemessenen Umfang unterstützen, wobei diese Unterstützung gemäß Ziffer 16 gesondert zu vergüten ist. Etwaige zusätzliche Leistungen zur Unterstützung des Kunden bei Vertragsbeendigung sind ebenfalls vergütungspflichtig und zwischen den Parteien separat zu vereinbaren.

---

[3] Art. 30 Abs. 2 lit. b) DORA
[4] Art. 30 Abs. 2 lit. b) DORA
[5] Art. 28 Abs. 5 bzw. 30 Abs. 3 lit. c) DORA
[6] Art. 30 Abs. 2 lit. d) DORA

6. IKT-BEZOGENER VORFALL[7]

6.1 Wenn ein IKT-bezogener Vorfall im Zusammenhang mit den Dienstleistungen auftritt, erklärt sich GFOS bereit, dem Kunden auf dessen Wunsch im angemessenen Umfang in Bezug auf diesen IKT-bezogenen Vorfall zu unterstützen.

6.2 GFOS wird dem Kunden auf Anfrage die bei GOFS vorhandenen Informationen, Angaben und Nachweise zur Verfügung stellen, die der Kunde benötigt, um gesetzlich für den Kunden bestehende Pflichten nach Maßgabe der Art. 17 bis 23 der DORA-VO (insbesondere Prüf-, Melde- und Dokumentationspflichten) zu erfüllen.

6.3 Die Unterstützung von GFOS im Rahmen von Ziffer 6.1 und Ziffer 6.2 ist gemäß Ziffer 16 gesondert zu vergüten.

7. KOOPERATION[8]

GFOS verpflichtet sich, auf Verlangen des Kunden mit den Zuständigen Behörden, die den Kunden beaufsichtigen, uneingeschränkt zusammenzuarbeiten. Diese Unterstützung von GFOS im Rahmen ist gemäß Ziffer 16 gesondert zu vergüten.

8. KÜNDIGUNGSRECHTE, ÄNDERUNG VON DIENSTLEISTUNGEN

8.1 Der Kunde hat das Recht, die betroffenen Relevanten Dienstleistungen mit einer Frist von dreißig (30) Tagen durch schriftliche Mitteilung an GFOS zu kündigen, wenn einer der folgenden Umstände vorliegt:[9]

(1) ein erheblicher Verstoß gegen Vertragsbedingungen durch GFOS, der von GFOS nicht innerhalb von dreißig (30) Tagen nach Erhalt einer Mitteilung, in der die Verletzung vollständig beschrieben und GFOS aufgefordert wird, diese zu beheben, behoben wurde;[10]

(2) ein erheblicher Verstoß von GFOS gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen;[11]

(3) nachweisliche Schwächen von GFOS in Bezug auf das allgemeines IKT-Risikomanagement von GFOS, insbesondere bei der Art und Weise, in der es die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Kundendaten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Kundendaten oder nicht personenbezogene Kundendaten handelt und diese Schwächen nicht innerhalb von dreißig (30) Tagen nach Erhalt einer Mitteilung, in der die Schwächen vollständig beschrieben und GFOS aufgefordert wird, diese zu beheben, behoben wurde;[12]

(4) eine Zuständige Behörde kann den Kunden infolge der Bedingungen des Vertrages oder der mit dem Vertrag verbundenen Umstände nicht mehr

---

[7] Art. 30 Abs. 2 lit. f) DORA
[8] Art. 30 Abs. 2 lit. g) DORA
[9] Art. 30 Abs. 2 lit. h), 28 Abs. 7 DORA
[10] Art. 28 Abs. 7 lit. a) DORA
[11] Art. 28 Abs. 7 lit. a) DORA
[12] Art. 28 Abs. 7 lit. c) DORA

wirksam beaufsichtigen;[13]

(5) Umstände, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen des Vertrages vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse von GFOS auswirken.[14]

8.2 Das in Ziffer 8.1 festgelegte Kündigungsrecht:

8.2.1 gilt nur für die Relevanten Dienstleistungen. Andere Dienstleistungen bleiben im Sinne einer Teilkündigung von der Kündigung unberührt; und

8.2.2 berührt nicht die sonstigen Rechte und Rechtsbehelfe von GFOS und dem Kunden, die sich aus dem Vertrag oder im Zusammenhang mit dem Vertrag ergeben können.

8.3 GFOS kann mit einer Frist von mindestens dreißig (30) Tagen Änderungen der Dienstleistungen (einschließlich der Service-Level und Standorte) vornehmen. Soweit GFOS eine solche Änderung der Dienstleistungen ohne vorherige Zustimmung des Kunden vornimmt und der Kunde vernünftigerweise davon ausgeht, dass eine solche Änderung wesentliche nachteilige Auswirkungen auf das IKT-Drittparteienrisikos und die Nutzung der Dienstleistungen durch den Kunden hat, kann der Kunde gegen diese Änderung Einspruch erheben (jeweils ein "Risikoeinwand"). Ein Risikoeinwand muss innerhalb von sieben (7) Tagen nach der Änderung schriftlich (Textform genügt) eingereicht werden und alle relevanten Informationen enthalten, die erforderlich sind, um zu prüfen, ob die Änderung wesentlich nachteilige Auswirkungen auf IKT-Drittparteienrisikos und die Nutzung der Dienstleistungen durch den Kunden hat. Nach Erhalt des Risikoeinwands werden sich die Parteien bemühen, die festgestellten Probleme partnerschaftlich zu lösen. Wenn die Parteien innerhalb von einundzwanzig (21) Tagen nach Zugang des Risikoeinwands bei GFOS nicht in der Lage sind, die Probleme zu lösen, und GFOS die Änderung nicht zurückgezogen hat, kann der Kunde die Relevanten Dienstleistungen mit einer Frist von drei (3) Monaten zum Quartalsende schriftlich kündigen.

9. SCHULUNGEN

9.1 GFOS wird alle GFOS-Mitarbeitenden, die an der Erbringung der Dienstleistungen beteiligt sind, jährlich zur Sensibilisierung für IKT-Sicherheit schulen.

9.2 Der Kunde kann verlangen, dass bestimmte GFOS-Mitarbeitende, die an der Erbringung der Dienstleistungen beteiligt sind, an den Schulungsprogrammen des Kunden zur Sensibilisierung für IKT-Sicherheit und zur digitalen operationalen Resilienz teilnehmen (zusammengefasst „Trainings“):[15]

9.2.1 Die Parteien werden gemeinsam bestimmen, welche GFOS-Mitarbeitenden an den Trainings teilnehmen und gemeinsam die damit verbundenen Zeitpläne und Terminplanung für die Durchführung festlegen.

9.2.2 Die Trainings werden, wenn möglich, als Online-Schulung durchgeführt.

9.2.3 Die Teilnahme von GFOS-Mitarbeitenden an den Trainings ist für den Kunden gemäß Ziffer 16 vergütungspflichtig.

---

[13] Art. 28 Abs. 7 lit. d) DORA
[14] Art. 28 Abs. 7 lit. b) DORA
[15] Art. 30 Abs. 2 lit. i) DORA

10. KRITISCHE ODER WICHTIGE FUNKTIONEN

Die in den nachstehenden Ziffern 11 bis 15 aufgeführten Klauseln gelten ausschließlich für KWF-Relevante Dienstleistungen.

11. GESCHÄFTSKONTINUITÄT UND UNTERBRECHUNG

11.1 GFOS wird:

11.1.1 dem Kunden auf Anfrage Berichte über die Leistungserbringung im Vergleich zu den vereinbarten Service-Level zur Verfügung stellen;[16]

11.1.2 den Kunden innerhalb einer angemessenen Frist über jede Entwicklung informieren, die sich wesentlich auf die Fähigkeit von GFOS, auswirken könnte, die Dienstleistungen zur Unterstützung für KWF-Relevante Dienstleistungen gemäß dem vertraglich vereinbarten Leistungsniveau wirksam bereitzustellen;[17] und

11.1.3 bei Nichterreichung des vereinbarten Leistungsniveaus so bald wie möglich geeignete Abhilfemaßnahmen ergreifen.[18]

11.2 GFOS wird[19]

11.2.1 einen Notfallplan zur Aufrechterhaltung des Geschäftsbetriebs implementieren und testen und über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung der Dienstleistungen bieten;

11.2.2 erforderlichenfalls den Notfallplan zur Aufrechterhaltung des Geschäftsbetriebs gemäß seinen Bestimmungen umsetzen; und

11.2.3 den Notfallplan zur Aufrechterhaltung des Geschäftsbetriebs regelmäßig überprüfen und (falls erforderlich) aktualisieren, um zu gewährleisten, dass er auf dem neuesten Stand bleibt.

12. BEDROHUNGSORIENTIERTER PENETRATIONSTEST (TLPT)[20]

12.1 Vorbehaltlich von Ziffer 12.2 ist GFOS verpflichtet, sich auf Verlangen des Kunden an den in den Art. 26, 27 DORA-VO genannten TLPT des Kunden zu beteiligen und daran uneingeschränkt mitzuwirken.[21] Der Kunde muss vor Umsetzung des TLPT detaillierte Informationen zur Verfügung stellen, um die relevanten Systeme, Prozesse oder Technologien zu identifizieren, die einem TLPT unterzogen werden sollen. Die Beteiligung und Mitwirkung von GFOS an einem TLPT des Kunden kann Folgendes umfassen:

12.1.1 Gewährung des Zugangs zu den für den TLPT erforderlichen Systemen, Instrumenten und Unterlagen;

12.1.2 Sicherstellung der Beteiligung und Zusammenarbeit aller relevanten Mitarbeitenden, einschließlich aller Vorkehrungen für die Geheimhaltung des TLPT;

---

[16] Art. 30 Abs. 3 lit. b) DORA
[17] Art. 30 Abs. 3 lit. b) DORA
[18] Art. 30 Abs. 3 lit. a) DORA
[19] Art. 30 Abs. 3 lit. c) DORA
[20] Art. 30 Abs. 3 lit. d) DORA
[21] Art. 30 Abs. 3 lit. d) DORA

12.1.3 Zusammenarbeit mit dem Kunden und den von ihm benannten Dritten in der Planungs-, Ausführungs- und Behebungsphase des TLPT;

12.1.4 Umsetzung aller erforderlichen Sicherheitsmaßnahmen oder Abhilfemaßnahmen, die während des TLPT-Prozesses ermittelt wurden; und

12.1.5 die Bereitstellung von Informationen und Unterlagen, die vom Kunden in angemessener Weise angefordert werden, um die Teilnahme und Mitarbeit von GFOS am TLPT-Prozess umzusetzen.

12.2 In jedem Fall vereinbaren die Parteien im Vorfeld eines TLPT wirksame Risikomanagementkontrollen, um die Risiken möglicher Auswirkungen auf die Dienstleistungen und die Leistungserbringung von GFOS gegenüber anderen Kunden zu minimieren.[22]

12.3 Der Kunde haftet gegenüber GFOS in vollem Umfang für die Handlungen und Unterlassungen seiner Tester, als ob es sich um Handlungen und Unterlassungen des Kunden handeln würde, und stellt sicher, dass alle Tester Vertraulichkeitsverpflichtungen unterliegen, die denen des Vertrags mindestens gleichwertig sind, und trifft alle angemessenen Vorkehrungen, um die Auswirkungen auf die Systeme von GFOS zu minimieren bzw. ganz auszuschließen.

12.4 Die Kosten der Beteiligung, Mitwirkung und Prüfung von GFOS bei dem TLPT im Rahmen dieser Ziffer 12 sind gemäß Ziffer 16 vergütungspflichtig.

13. ÜBERWACHUNG

13.1 Vorbehaltlich der Ziffer 13.3 gewährt GFOS dem Kunden, einem entsprechend beauftragten Dritten und der Zuständigen Behörde (jeweils "überwachende Stelle") uneingeschränkte Zugangs-, Inspektions- und Auditrechte sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort, wenn diesen für die Geschäftstätigkeit von GFOS entscheidende Bedeutung zukommt, wobei die tatsächliche Ausübung dieser Rechte nicht durch andere vertragliche Vereinbarungen oder Umsetzungsrichtlinien behindert oder eingeschränkt wird. Diese Rechte gelten jeweils in dem Maße, wie es die überwachende Stelle vernünftigerweise für die Überwachung der Dienstleistungen für erforderlich hält.[23]

13.2 GFOS verpflichtet sich zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den Zuständigen Behörden, der federführenden Aufsichtsbehörde, dem Kunden oder einem beauftragten Dritten durchgeführt werden.[24]

13.3 Vorbehaltlich Ziffer 13.4 übt der Kunde die in Ziffer 13.1 genannten Rechte auch in Bezug auf von ihm beauftragte Dritte nach Maßgabe der folgenden Bestimmungen aus:

13.3.1 Der Kunde übt die Rechte auf der Grundlage eines risikobasierten Ansatzes aus und hält sich dabei an allgemein anerkannte Auditstandards;[25]

13.3.2 der Kunde teilt GFOS den Umfang, die Verfahren, die Häufigkeit sowie die zu prüfenden Bereiche von Audits und Inspektionen mit;[26]

13.3.3 der Kunde teilt GFOS mit angemessener Frist (gemessen an der Art und dem Umfang der beantragten Prüfung) die Durchführung von Audits und Inspektionen

[22] Art. 26 Abs. 5 DORA
[23] Art. 30 Abs. 3 lit. e) i) DORA
[24] Art. 30 Abs. 3 lit. e) iii) DORA
[25] Art. 28 Abs. 6 DORA
[26] Art. 28 Abs. 6 und Art. 30 Abs. 3 lit. e) iv) DORA

mit, bevor er sein Recht auf Zugang vor Ort ausübt, es sei denn, dies ist aufgrund einer Not- oder Krisensituation nicht möglich oder eine solche Mitteilung würde den Prüfungszweck vereiteln; und

13.3.4 wenn die Rechte anderer Kunden von GFOS beeinträchtigt werden, vereinbaren die Parteien alternative Bestätigungsniveaus.[27]

13.4 Die Regelungen in Ziffer 13.3 schränken die Rechte der Zuständigen Behörden in keiner Weise ein, wenn diese den Anforderungen der DORA-VO zuwiderlaufen.

13.5 Die im Rahmen dieser Ziffer 13 von GFOS zu erbringenden Unterstützungsleistungen sind gemäß Ziffer 16 vergütungspflichtig.

14. TRANSITION

14.1 Im Sinne dieser Ziffer 14 bedeutet "Übergangszeitraum" ein vom Kunden schriftlich festgelegter Zeitraum, der mit dem Datum der Beendigung des Vertrags beginnt und nicht länger als drei Monate über dieses Datum hinausgeht, es sei denn, dass GFOS schriftlich einem längeren Zeitraum zustimmt.

14.2 Während des Übergangszeitraums verpflichtet sich GFOS nach schriftlicher Beauftragung durch den Kunden:[28]

14.2.1 die Dienstleistungen während des Übergangszeitraums in der gleichen Weise weiter zu erbringen, wie dies vor dem Übergangszeitraum geschuldet war, wobei alle einschlägigen Bestimmungen des Vertrags während des Übergangszeitraums fortgelten; und

14.2.2 dem Kunden die Unterstützung zu gewähren, die er benötigt, um zu einem anderen IKT-Drittdienstleister zu wechseln oder auf interne Lösungen umzustellen, die der Komplexität der erbrachten Dienstleistung entsprechen.

14.3 Der Ausstiegszeitraum gemäß Ziffer 5 beginnt in den Fällen dieser Ziffer 14 mit dem Ende des Übergangszeitraums.

14.4 Die Vergütung für die in dieser Ziffer 14 geregelten Unterstützungsleistungen werden dem Kunden wie nachstehend geregelt in Rechnung gestellt:

14.4.1 die fortgesetzte Erbringung der Dienstleistungen gemäß Ziffer 14.2.1 wird auf derselben vertraglichen Grundlage (d. h. auf der Grundlage derselben Gebühren, Kosten und Auslagen oder derselben Berechnungsgrundlage) wie im Zeitraum unmittelbar vor der Beendigung des Vertrags vergütet. Diese Vergütung ist ab dem Datum der Vertragsbeendigung bis zum Ende des Übergangszeitraums in voller Höhe zu zahlen; und

14.4.2 die Unterstützung gemäß Ziffer 14.2.2 wird dem Kunden gemäß Ziffer 16 in Rechnung gestellt.

15. UNTERVERGABE VON AUFTRÄGEN

Die Verpflichtungen von GFOS

15.1 GFOS ist

[27] Art. 30 Abs. 3 lit. e) ii) DORA
[28] Art. 30 Abs. 3 lit. f) DORA

15.1.1 für die Erbringung der untervergebenen Dienstleistungen verantwortlich; GFOS ist dabei für alle Handlungen oder Unterlassungen jedes Unterauftragnehmers bei der Erbringung der untervergebenen Dienstleistungen so verantwortlich, als wären es die eigenen Handlungen oder Unterlassungen;[29]

15.1.2 verpflichtet, alle untervergebenen Dienstleistungen, die KWF-Relevante Dienstleistungen sind oder wesentliche Teile davon unterstützen, zu überwachen, um sicherstellen, dass die vertraglichen Verpflichtungen gegenüber dem Kunden erfüllt werden;[30]

15.1.3 verpflichtet, seine Unterauftragnehmer, die KWF-Relevante Dienstleistungen erbringen oder wesentliche Teile davon unterstützen, zu überwachen und dem Kunden darüber zu berichten;[31]

15.1.4 verpflichtet, den Kunden, sofern relevant, über den Standort der von den Unterauftragnehmern verarbeiteten oder gespeicherten Kundendaten gemäß Ziffer 3.3 zu informieren;[32] und

15.1.5 verpflichtet, Ziffer 11 und Ziffer 14.2.2 einhalten, um die Kontinuität der von GFOS (und seinen Unterauftragnehmern) erbrachten Dienstleistungen zu gewährleisten.

Vereinbarungen mit Unterauftragnehmern

15.2 GFOS muss mit jedem seiner Unterauftragnehmer, der Dienstleistungen erbringt, die KWF-Relevante Dienstleistungen sind oder wesentliche Teile davon unterstützen, eine schriftliche Vereinbarung abschließen und diese Vereinbarungen müssen vorsehen, dass (in Bezug auf die untervergebenen Elemente der Dienstleistungen):[33]

15.2.1 Überwachungs- und Berichtspflichten des Unterauftragnehmers gegenüber GFOS bestehen;[34]

15.2.2 der Unterauftragnehmer Notfallpläne implementiert und testet, die den Anforderungen von Ziffer 11 (soweit sie für den Umfang der untervergebenen Dienstleistungen relevant sind) gleichwertig sind;[35]

15.2.3 der Unterauftragnehmer über Sicherheitsmaßnahmen, -instrumente und -strategien verfügt, die den in Ziffer 4 geforderten gleichwertig sind;[36] und

15.2.4 der Unterauftragnehmer Zugangs-, Inspektions- und Prüfungsrechte gewährt, die den in Ziffer 13 genannten entsprechen.[37]

Identifizierung und Änderung von Unteraufträgen

15.3 Die Unterauftragnehmer, die zum Zeitpunkt der Vereinbarung dieser Anlage an der Erbringung der Dienstleistungen beteiligt sind, sind in Anhang 0 aufgeführt.[38]

[29] Art. 4 Abs. 1 lit. a) Unterauftragsvergabe RTS
[30] Art. 4 Abs. 1 lit. b) Unterauftragsvergabe RTS
[31] Art. 4 Abs. 1 lit. c) Unterauftragsvergabe RTS
[32] Art. 4 Abs. 1 lit. e) Unterauftragsvergabe RTS
[33] Art. 4 Abs. 1 Unterauftragsvergabe RTS
[34] Art. 4 Abs. 1 lit. f) Unterauftragsvergabe RTS
[35] Art. 4 Abs. 1 lit. g) Unterauftragsvergabe RTS
[36] Art. 4 Abs. 1 lit. h) Unterauftragsvergabe RTS
[37] Art. 4 Abs. 1 lit. i) Unterauftragsvergabe RTS
[38] Art. 5 Abs. 1 lit. a) Unterauftragsvergabe RTS

15.4 GFOS wird die Liste der identifizierten Unterauftragnehmer während der Laufzeit des Vertrags[39] aktualisieren, indem GFOS den Kunden gemäß dieser Anlage über Änderungen informiert.

15.5 GFOS kann die Vereinbarungen über die Vergabe von Unteraufträgen von Zeit zu Zeit ändern, vorausgesetzt, dass GFOS bei jeder wesentlichen Änderung (einschließlich der Ernennung eines neuen Unterauftragnehmers für die Erbringung der Dienstleistungen, der Beendigung oder des Ersatzes eines bestehenden Unterauftragnehmers oder einer wesentlichen Änderung der im Rahmen eines bestehenden Unterauftragsvertrags erbrachten Dienstleistungen) verpflichtet ist:

15.5.1 nur dann eine solche Änderung vorzunehmen, wenn sie dem Kunden mindestens dreißig (30) Tage im Voraus angekündigt wurde. Eine solche Änderung unterliegt dem in Ziffer 8.3 dargelegten Verfahren, das dem Kunden die Möglichkeit gibt, Einspruch zu erheben und schließlich den Vertrag zu kündigen (wie in Ziffer 8.3 weiter ausgeführt, wobei "Änderung der Dienstleistungen" im Sinne von Ziffer 8.3 auch "wesentliche Änderungen bei der Vergabe von Unteraufträgen" bedeutet); und

15.5.2 nach Möglichkeit mit dem Kunden zusammenarbeiten, um ihn bei der Bewertung der Auswirkungen der vorgeschlagenen Änderung auf die Risiken für den Kunden zu unterstützen.

15.6 Vor der Beauftragung eines Unterauftragnehmers bewertet GFOS alle relevanten Risiken, einschließlich der IKT-Risiken, die verbunden sind mit:

15.6.1 dem Sitz des aktuellen oder potenziellen Unterauftragnehmers und seiner Muttergesellschaft und dem Ort, von dem aus die Dienstleistungen erbracht werden sollen;[40] oder

15.6.2 dem Ort, an dem die Kundendaten durch den Unterauftragnehmer verarbeitet oder gespeichert werden sollen.[41]

15.7 Auf Anfrage gewährt GFOS dem Kunden Einsicht in die Vertragsunterlagen zwischen GFOS und einem Unterauftragnehmer und Performance-Zahlen, soweit der Kunde diese vernünftigerweise benötigt im Hinblick auf sein Überwachungsrecht und seinen Pflichten aus der delegierten Verordnung (EU) 2024/1773.[42]

15.8 Die im Rahmen dieser Ziffer 15 von GFOS zu leistenden Unterstützungsleistungen sind gemäß Ziffer 16 vergütungspflichtig.

16. Vergütung

16.1 Sofern nicht anders vereinbart und vorbehaltlich von Ziffer 16.2, sind alle Schulungs-, Mitwirkungs- und Unterstützungsleistungen von GFOS im Rahmen dieser Anlage (einschließlich der Ziffern 5.3, 6, 7, 9, 12, 13, 14 und 15) vergütungspflichtig und werden dem Kunden wie folgt in Rechnung gestellt:

16.1.1 Für die von GFOS-Mitarbeitenden im Zusammenhang mit diesen Tätigkeiten aufgewendete Zeit schuldet der Kunde eine Vergütung nach Aufwand in Form von Tagessätzen gemäß der zum Abrechnungszeitpunkt gültigen Preisliste von GFOS.

---

[39] Art. 5 Abs. 1 lit. b) Unterauftragsvergabe RTS
[40] Art. 4 Abs. 1 lit. d) Unterauftragsvergabe RTS
[41] Art. 4 Abs. 1 lit. e) Unterauftragsvergabe RTS
[42] Art. 5 Abs. 4 Unterauftragsvergabe RTS

Die Abrechnung erfolgt monatlich nachträglich nach Leistungserbringung. Reisekosten, Materialkosten, Spesen und/oder sonstige Nebenkosten sind nicht in den Tagessätzen enthalten und werden zusätzlich in Rechnung gestellt.

16.1.2 Alle sonstigen Kosten oder Ausgaben, die GFOS im Zusammenhang mit den in Ziffer 16.1 aufgeführten Tätigkeiten entstehen (z. B. wenn Produkte oder Dienstleistungen eines Dritten, einschließlich der Unterauftragnehmer von GFOS, benötigt werden), werden auf der Grundlage der Kosten für GFOS (ohne Aufschlag durch GFOS) an den Kunden nach Anfall weiter berechnet.

16.2 GFOS wird dem Kunden keine Kosten für Schulungs-, Mitwirkungsmaßnahmen- und Unterstützungsmaßnahmen o.ä. im Rahmen dieser Anlage in Rechnung stellen, soweit GFOS bereits verpflichtet ist, diese Maßnahmen gemäß den bestehenden Vertragsbedingungen durchzuführen.

16.3 GFOS wird auf Anfrage des Kunden Kostenvoranschläge für die nach dieser Ziffer 16 zu vergütenden Dienstleistungen und zu erstattenden Kosten vorlegen und den Kunden laufend vor Überschreitung eines Kostenvoranschlags informieren.

17. ON-PREMISE SOFTWARE, NUTZUNG VON LEISTUNGEN VON HYPERSCALERN

17.1 Soweit die Dienstleistungen die Bereitstellung und Nutzung von On-Premise-Software umfassen (d.h. Software, die vom Kunden selbst betrieben und gehostet wird), gelten die in dieser Anlage dargelegten Verpflichtungen nur in dem Umfang, der für die Bereitstellung und den Support der On-Premise-Software gilt:

17.1.1 Ziffer 3.3 gilt nur insoweit, als die Systeme von GFOS Kundendaten hosten oder verarbeiten;

17.1.2 Ziffer 4 gilt nur für die Systeme von GFOS, soweit sie Kundendaten hosten oder verarbeiten. Der Kunde ist für die Sicherheit der von ihm gehosteten Umgebung selbst verantwortlich;

17.1.3 Ziffer 5 findet keine Anwendung; und

17.1.4 Ziffer 12 findet keine Anwendung.

17.2 Soweit der Kunde zur Nutzung der Dienstleistungen selbständig Dritte, insbesondere Hyperscaler, z.B. zum Hosting der On-Premise-Software beauftragt, ist GFOS nicht für die Einhaltung der Anforderungen der DORA-VO durch den Dritten/Hyperscaler verantwortlich.

ANHANG - Relevante Dienstleistungen

Name der relevanten Dienstleistungen	Relevante Dienstleistungen Beschreibung	KWF (kritische oder wichtige Funktion)

ANHANG - Standorte

Dienstleistungen/Kundendaten	Standort

[Für Unterauftragnehmer sind die Dienstorte in 0. ANHANG - aufgeführt].

ANHANG - Unterauftragnehmer

Unterauftragnehmer und Anschrift / Standort	Beschreibung von untervergeben Dienstleistungen und deren Umfang