

Annex

„Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector”

Einleitung

Arvato Systems ist ein Dienstleister für Kunden, die der staatlichen Aufsicht durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und die Deutsche Bundesbank (Bundesbank) unterliegen.

Aufgrund dieser Umstände haben Versicherungsgesellschaften, Banken, Zahlungsinstitute und andere Finanzdienstleister (im Folgenden als „regulierte Unternehmen“ bezeichnet) besondere Anforderungen an die Auslagerung von Dienstleistungen an Dritte.

Die Anforderungen, die regulierte Unternehmen an Arvato Systems stellen, sind im Folgenden aufgeführt und müssen im Falle einer Auslagerung über die gesamte Dienstleistungskette hinweg eingehalten werden – auch von den Subunternehmern von Arvato Systems. In solchen Fällen hat der Subunternehmer seine Dienstleistungen daher so zu erbringen, dass Arvato Systems diese Anforderungen in Bezug auf die Dienstleistungen des Subunternehmers erfüllen kann.

In Bezug auf die nachstehend aufgeführten Anforderungen ist Folgendes zu beachten:

- „Kunde“ bezeichnet das regulierte Unternehmen, für das Arvato Systems Dienstleistungen erbringt, die als Outsourcing gelten. In der Beziehung zwischen Arvato Systems und Subunternehmern hat Arvato Systems gegenüber dem Subunternehmer ebenfalls die Rechte des Kunden; Arvato Systems kann diese Rechte für sich selbst und/oder das regulierte Unternehmen geltend machen. Darüber hinaus bleibt das regulierte Unternehmen berechtigt, die Rechte des Kunden direkt gegenüber dem Subunternehmer geltend zu machen.
- „Dienstleister“ bezeichnet Arvato Systems, das für ein reguliertes Unternehmen Dienstleistungen erbringt, die als Outsourcing gelten. In der Beziehung zwischen Arvato Systems und Subunternehmern hat der Subunternehmer die Pflichten des Dienstleisters.

Annex „Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector”

1 Pflichten des Dienstleisters

Der Dienstleister ist verpflichtet, im Rahmen der Erbringung der Dienstleistungen gemäß dem Vertrag Folgendes zu tun:

- 1.1. Der Dienstleister verfügt über angemessene Standards für die Informationssicherheit und wendet die neuesten und höchsten Qualitätsstandards für die Informationssicherheit an, wobei insbesondere die vom Kunden implementierten Informationssicherheitsstandards vom Dienstleister einzuhalten sind (Sicherheitstechnische und organisatorische Maßnahmen des Kunden). ¹
- 1.2. Wenn der Kunde Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen Betriebsstabilität anbietet und vom Personal des Dienstleisters die Teilnahme daran verlangt, nimmt der Dienstleister an diesen Schulungen teil. Die Teilnahme an den Schulungen ist kostenlos, jedoch gilt die Schulungszeit nicht als abrechnungsfähige Zeit. Das Personal des Dienstleisters ist verpflichtet, die Inhalte der Schulungen vertraulich zu behandeln. Auf Wunsch des Kunden legt der Dienstleister dem zuständigen Personal entsprechende Nachweise über die Teilnahme an Schulungen zu Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz vor, die vom Dienstleister selbst oder von Dritten durchgeführt wurden. ²
- 1.3. Darüber hinaus verpflichtet sich der Dienstleister und/oder seine Subunternehmer – je nachdem, für wen die Zertifizierung für die Erbringung der jeweiligen Dienstleistung erforderlich ist – über die folgenden Zertifizierungen zu verfügen, diese einschließlich ihrer Nachfolgezertifizierungen aufrechtzuerhalten und dem Kunden auf Anfrage Nachweise über die bestehenden Zertifizierungen vorzulegen: (i) ISO 27001 und (ii) ISAE 3402. Der Geltungsbereich der Zertifizierungen muss in jedem Fall alle Teile der Organisation des Dienstleisters umfassen, die an der Erbringung

¹ Diese Klausel setzt Art. 28 Abs. 5 der DORA-Verordnung um.

² Diese Klausel setzt Art. 30 Abs. 2 Buchstabe i der DORA-Verordnung um.

der vereinbarten Dienstleistungen beteiligt sind. Der Dienstleister muss diese Verpflichtung seinen Subunternehmern durch einen schriftlichen Vertrag auferlegen.³

Sofern und soweit für die Erbringung der Dienstleistung in Zukunft weitere Zertifizierungen erforderlich sind, sind diese in jedem Fall vom jeweiligen Dienstleister zu erwerben. Darüber hinaus kann der Kunde die Einholung weiterer Zertifikate verlangen, wobei der Dienstleister die Kosten für die zur Erbringung der Dienstleistung erforderlichen Zertifizierungen zu tragen hat. Die Kosten für zusätzliche Zertifizierungen trägt der Kunde, es sei denn, der Dienstleister verfügt bereits über diese.

2 Unterstützung bei IKT-bezogenen Vorfällen ⁴

- 2.1. Der Dienstleister informiert den Kunden unverzüglich, proaktiv und schriftlich über IKT-bezogene Vorfälle und zahlungsbezogene Betriebs- oder Sicherheitsvorfälle im Sinne der DORA-Verordnung, die mit den Dienstleistungen des Dienstleisters und/oder seiner Unterauftragnehmer in Zusammenhang stehen.
- 2.2. Der Dienstleister unterstützt den Kunden im Falle eines IKT-bezogenen Vorfalls im Sinne der DORA-Verordnung im Zusammenhang mit den Dienstleistungen des Dienstleisters.
- 2.3. Der Dienstleister berechnet keine zusätzlichen Kosten für die Unterstützung im Falle eines IKT-bezogenen Vorfalls.

3 Einsatz von Subunternehmern ⁵

- 3.1. Der Dienstleister erbringt die Dienstleistungen im Rahmen des Vertrags grundsätzlich selbst. Beabsichtigt der Dienstleister, Dritte („Subunternehmer“) für die Erbringung von Dienstleistungen einzusetzen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, bedarf dies der vorherigen schriftlichen Zustimmung des Kunden.
- 3.2. Eine Liste der aktuellen Subunternehmer muss vom Dienstleister in **Anhang 1** angegeben werden.
- 3.3. Der Einsatz von Subunternehmern für (Teil-)Leistungen aus dem Vertrag ist nicht zulässig, wenn:
 - 3.3.1. der Subunternehmer seinen Sitz außerhalb des Europäischen Wirtschaftsraums hat;
 - 3.3.2. die Auslagerung zu einer Datenübermittlung außerhalb des Europäischen Wirtschaftsraums führt, es sei denn, dies wurde vom Kunden vorbehaltlich etwaiger Bedingungen ausdrücklich im Voraus schriftlich genehmigt; In jedem Fall müssen die besonderen Anforderungen der DSGVO für Datenübermittlungen in Drittländer (Art. 44 ff.) erfüllt sein, wie z. B. die EU-Standardvertragsklauseln (SCC) oder andere geeignete Garantien.
 - 3.3.3. der Unterauftragnehmer mit dem Kunden im Wettbewerb steht.
- 3.4. Der Dienstleister muss den Kunden schriftlich mit einer angemessenen Vorlaufzeit von mindestens 60 Tagen informieren und alle wesentlichen Unterlagen aus der Sorgfaltsprüfung im Sinne von Abschnitt 3.7 in ausreichender Qualität vorlegen, insbesondere die Einzelheiten zum Umfang der geplanten Inanspruchnahme des Subunternehmers oder der Änderung und die Qualifikation des Subunternehmers („Benachrichtigung“). Der Kunde ist berechtigt, der (geänderten) Inanspruchnahme des Subunternehmers zu widersprechen, wenn dies wesentliche Interessen des Kunden beeinträchtigen könnte. Dies ist der Fall, wenn dem Subunternehmer Zugang zu personenbezogenen Daten gewährt wird, bei erheblichen nachteiligen Auswirkungen auf das Outsourcing-Verhältnis, bei einer Erhöhung des Risikos oder aufgrund regulatorischer Anforderungen. Widerspricht der Kunde einer rechtzeitig angekündigten (Änderung der) Inanspruchnahme eines Subunternehmers nicht innerhalb von 60 Tagen nach Erhalt der Mitteilung, gilt

³ Dieser Punkt setzt Art. 8 Abs. 2 Buchstabe c DeIVO (EU) 2024/1773 um (RTS, in dem der detaillierte Inhalt der Richtlinie zu vertraglichen Vereinbarungen über die Nutzung von IKT-Diensten, die kritische oder wichtige Funktionen unterstützen und von externen IKT-Dienstleistern bereitgestellt werden, festgelegt ist).

⁴ Dieses Kapitel setzt Art. 30 Abs. 2 Buchstabe f der DORA-Verordnung um.

⁵ Der folgende Abschnitt 3.1 setzt Randnummer 37 Buchstabe e der EIOPA-Leitlinien (EIOPA-BoS-20-002) und Art. 274 Abs. 4 Buchstabe k DeIVO 2015/35 um. Darüber hinaus ändert dieses Kapitel Artikel 7 Absatz 1, Artikel 3 Absatz 1, Artikel 4 und Artikel 6 des Konsultationspapiers zu den RTS, um die Elemente zu präzisieren, die ein Finanzunternehmen bei der Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, gemäß Artikel 30 Absatz 5 der DORA-Verordnung („RTS zur Vergabe von Unteraufträgen“) festlegen und bewerten muss.

- dies als Zustimmung. Wird rechtzeitig Widerspruch eingelegt, ist der Dienstleister nicht berechtigt, die geplante Auslagerung oder Änderung durchzuführen.
- 3.5. Im Falle von Änderungen des zugelassenen Subunternehmers oder seiner Dienstleistungen, die zu einer erheblichen Erhöhung des Risikos für den Kunden führen, hat der Kunde das Recht, Änderungen an den vorgeschlagenen Änderungen der Untervergabe zu verlangen, bevor diese umgesetzt werden.
- 3.6. Der Kunde kann die Zustimmung und Genehmigung eines Subunternehmers aus wichtigem Grund jederzeit in der Zukunft widerrufen.
- 3.7. Im Zusammenhang mit dem Einsatz von Subunternehmern muss der Dienstleister die folgenden Mindestanforderungen erfüllen, bevor er den Subunternehmer einsetzt, der kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützt, und zwar fortlaufend: ⁶
- Implementierung und Durchführung eines Due-Diligence-Prozesses, der sicherstellt, dass der Dienstleister die Eignung des Subunternehmers für die Erbringung von Dienstleistungen beurteilen kann. Die Due Diligence muss vor der Beauftragung des Subunternehmers durchgeführt werden. Ihr Umfang muss den Anforderungen der technischen Regulierungsstandards gemäß Art. 28 Abs. 10 und Art. 30 Abs. 5 der DORA-Verordnung entsprechen und unter anderem Folgendes umfassen: Bewertung der Fähigkeiten, Fachkenntnisse und finanziellen, personellen und technischen Ressourcen des Subunternehmers (auch durch Teilnahme an der operativen Berichterstattung und operativen Tests, wie vom Kunden verlangt); Bewertung der Informationssicherheitsstandards, der Organisationsstruktur, des Risikomanagements und der internen Kontrollen.
 - Bewertung aller Risiken, einschließlich IKT-Risiken, die mit dem Standort des Subunternehmers und gegebenenfalls seiner Muttergesellschaft sowie dem Standort, von dem aus die untervergebene Dienstleistung erbracht wird, verbunden sind (siehe Anhang I); und Bereitstellung relevanter Unterlagen zu dieser Risikobewertung auf Anfrage des Kunden;
 - Festlegung der Überwachungs- und Berichtspflichten des Subunternehmers, die dieser gegenüber dem Dienstleister und damit auch gegenüber dem Kunden zu erfüllen hat;
 - Kontinuierliche Erbringung der Dienstleistung, auch wenn ein Subunternehmer seine Dienstleistungsstandards oder andere vertragliche Verpflichtungen nicht erfüllt; und
 - Kontinuierliche Einhaltung der IKT-Sicherheitsstandards und gegebenenfalls der zusätzlichen Sicherheitsmerkmale durch den Subunternehmer gemäß den technischen Regulierungsstandards gemäß Art. 28 Abs. 10 DORA-Verordnung.
- 3.8. Der Dienstleister muss alle sich aus dem Vertrag und dieser Zusatzvereinbarung ergebenden Verpflichtungen jedem Subunternehmer im Rahmen der Beauftragung des jeweiligen Subunternehmers schriftlich auferlegen. Der Vertrag mit dem Subunternehmer muss sicherstellen, dass der Kunde und die zuständigen Behörden ihre Informations-, Prüfungs- und Weisungsrechte direkt gegenüber dem Subunternehmer ausüben können. Der Dienstleister muss die fortlaufende Einhaltung des Vertrags und dieser Zusatzvereinbarung durch den Unterauftragnehmer kontinuierlich überwachen und dies auf Verlangen des Kunden nachweisen. ⁷
- 3.9. Der Dienstleister muss den Kunden unverzüglich, proaktiv und schriftlich über alle Entwicklungen bei den Subunternehmern informieren, die einen wesentlichen Einfluss auf die ordnungsgemäße Erbringung der Leistungen aus dem Vertrag und dieser Zusatzvereinbarung haben könnten. Der Dienstleister haftet für alle Subunternehmer wie für seine eigenen Handlungen. Darüber hinaus bleiben die Verpflichtungen und Verantwortlichkeiten des Dienstleisters aus dem Vertrag und dieser Zusatzvereinbarung von einer Untervergabe unberührt. ⁸

4 Standorte der Leistungserbringung und Datenverarbeitung ⁹

- 4.1. Das Land, in dem der Dienstleister und seine zugelassenen Subunternehmer die Dienstleistungen erbringen und in dem sie die Daten speichern und verarbeiten, muss in Anhang 1 dokumentiert werden. Beabsichtigen der

⁶ Dieser Abschnitt 3.3 setzt die Artikel 3 und 4 des Konsultationspapiers zu den Entwürfen der RTS zur Untervergabe um.

⁷ Dieser Punkt setzt Art. 3 Abs. 1 Buchstabe c und Art. 4 Buchstabe i der RTS zur Untervergabe um.

⁸ Dieser Punkt setzt Randnummer 80 Buchstabe c EIOPA-BoS-20/600, Artikel 274 Absatz 4 Buchstaben c und I DelVO 2015/35 und Artikel 30 Absatz 3 Buchstabe b der DORA-Verordnung um.

⁹ Dieser Abschnitt setzt Randnummer 37 Buchstabe f EIOPA-BoS-20-002 und Artikel 30 Absatz 2 Buchstabe b DORA-Verordnung um.

Dienstleister oder der Subunternehmer, diese Orte zu ändern, muss der Kunde vorab informiert werden. Zusätzlich zu dieser Informationspflicht muss der Dienstleister die in Abschnitt 4.2 genannten Verpflichtungen erfüllen.

- 4.2. Die vollständige oder teilweise Verlegung eines Erfüllungsortes, eines Ortes der Datenspeicherung und -verarbeitung oder des Sitzes durch den Dienstleister oder den Unterauftragnehmer bedarf stets der vorherigen schriftlichen Zustimmung des Kunden.

5 Zugang zu Daten

- 5.1. Im Falle einer Insolvenz, Auflösung, Einstellung der Geschäftstätigkeit des Dienstleisters oder Beendigung des Vertrags oder dieser Zusatzvereinbarung ist der Kunde berechtigt, unverzüglich auf seine Daten zuzugreifen.
- 5.2. Der Dienstleister wird den Kunden umfassend unterstützen, ihm uneingeschränkten Zugang gewähren und sicherstellen, dass die Daten des Kunden in einem vom Kunden festgelegten, leicht zugänglichen Format wiederhergestellt und zurückgegeben werden.¹⁰

6 Notfallmaßnahmen

- 6.1. Der Dienstleister implementiert und testet seine Notfallpläne. Darüber hinaus verfügt der Dienstleister über Maßnahmen, Instrumente und Richtlinien für die IKT-Sicherheit, die ein angemessenes Sicherheitsniveau für die Erbringung von Dienstleistungen durch den Kunden gemäß dessen rechtlichem Rahmen gewährleisten.
- 6.2. Der Dienstleister dokumentiert die Durchführung der Tests der Notfallpläne und stellt diese Dokumentation dem Kunden auf Anfrage unverzüglich zur Verfügung.¹¹

7 Service Level¹²

- 7.1. Es gelten die in der Vereinbarung festgelegten Service Levels, die eine effektive Überwachung der Erbringung von Dienstleistungen durch den Kunden ermöglichen. Die Service Levels werden vom Dienstleister und vom Kunden bei Bedarf überprüft, um sicherzustellen, dass sie angesichts der Weiterentwicklung der technischen Standards angemessen sind, und werden bei Bedarf angepasst oder ergänzt. Der Kunde kann in jedem Fall entsprechende Anpassungen und Ergänzungen der Service Levels verlangen, wenn die vereinbarte Servicequalität nicht erreicht wird. Der Dienstleister kommt den entsprechenden Anforderungen des Kunden zur Anpassung oder Änderung der Service Levels unverzüglich nach und setzt auch die vom Kunden ergriffenen geeigneten Korrekturmaßnahmen unverzüglich um, wenn die vereinbarte Servicequalität nicht erreicht wird.
- 7.2. Der Dienstleister muss den Kunden unverzüglich, proaktiv und schriftlich über alle Entwicklungen informieren, die einen wesentlichen Einfluss auf die ordnungsgemäße Erbringung der Dienstleistungen und/oder die damit verbundenen Aktivitäten und Prozesse gemäß den vereinbarten Service Levels haben könnten.¹³

8 Informations- und Prüfungsrechte¹⁴

- 8.1. Der Dienstleister gewährt dem Kunden, den beauftragten Dritten (z. B. internen und externen Prüfern), den Aufsichtsbehörden und -stellen sowie der Abwicklungsbehörde des Kunden während der Laufzeit des Vertrags und nach dessen Beendigung die folgenden Informations- und Prüfungsrechte in Bezug auf die Dienstleistungen des Dienstleisters und seiner Unterauftragnehmer:
- Uneingeschränkte Zugangs-, Einsichts-, Anweisungs- und Prüfungsrechte, einschließlich des uneingeschränkten Zugangs zu allen Geschäftsräumen, einschließlich aller relevanten Geräte, Systeme,

¹⁰ Grundsätzlich geregelt in Margin Nr. 37 Buchstabe n EIOPA-BoS-20-002, jedoch konkretisiert durch Art. 30 Abs. 2 Buchstabe d DORA-Verordnung (insbesondere hinsichtlich der Form der Datenübermittlung).

¹¹ Dieser Punkt setzt Randnummer 80 Buchstabe b EIOPA-BoS-20/600 und Randnummer 37 Buchstabe l EIOPA-BoS-20-002 sowie Art. 30 Abs. 3 Buchstabe c und Art. 28 Abs. 8 DORA-Verordnung um.

¹² Dieses Kapitel setzt Randnummer 80 Buchstabe a der EIOPA-Leitlinien zur IKT-Sicherheit (im Folgenden „EIOPA-BoS-20/600“), Randnummer 37 Buchstabe i EIOPA-BoS-20-002, Art. 274 Abs. 4 Buchstabe f DeIVO 2015/35 und Art. 30 Abs. 2 Buchstabe e und Abs. 3 Buchstabe a DORA-Verordnung.

¹³ Dieser Punkt setzt Randnummer 80 Buchstabe c EIOPA-BoS-20/600 und Art. 30 (3) Buchstabe b DORA-Verordnung um.

¹⁴ Dieses Kapitel setzt Randnummer 80 Buchstabe d EIOPA-BoS-20/600, Art. 274 Abs. 4 Buchstabe h und j DeIVO 2015/35, Randnummer 37 Buchstabe h und m EIOPA-BoS-20-002 und Art. 30 Abs. 3 Buchstabe e UAbs i) bis iv) und Art. 28 Abs. 6 DORA-Verordnung um. Es setzt außerdem Art. 8 Abs. 2 DeIVO (EU) 2024/1773 (RTS zum Testen) um.

Netzwerke, Informationen und Daten, die für die Erbringung der vertraglich vereinbarten Dienstleistungen verwendet werden, einschließlich in Verbindung mit Finanzinformationen, Personal und den externen Wirtschaftsprüfern des Dienstleisters; sowie Zugang zu Mitarbeitern, Dokumenten, Datenspeichern, Geschäftsräumen und Systemen des Dienstleisters und seiner Subunternehmer sowie die Bereitstellung und Übermittlung von Informationen und Dokumenten. Insbesondere gewährt der Dienstleister dem Kunden, den Prüfungs-, Aufsichts- und Abwicklungsgremien und -behörden uneingeschränkten und ungehinderten Zugang zu allen Aufzeichnungen, Informationen und Daten im Zusammenhang mit den Dienstleistungen im Rahmen des Vertrags, insbesondere zu denen, die erforderlich sind, um sicherzustellen, dass die Dienstleistungen den regulatorischen und datenschutzrechtlichen Anforderungen entsprechen.

- Gewährung uneingeschränkter Inspektions- und Prüfungsrechte im Zusammenhang mit dem Vertrag, um die laufende Überwachung der Vertragseinhaltung zu ermöglichen und die Einhaltung der gesetzlichen Anforderungen sicherzustellen, sowie uneingeschränkte Zusammenarbeit in dieser Hinsicht.
- das Recht, vor Ort Kopien von relevanten Dokumenten anzufertigen, wenn diese für die Geschäftstätigkeit des Dienstleisters von entscheidender Bedeutung sind;
- das Recht, alternative Sicherheitsstufen zu vereinbaren, wenn die Rechte anderer Kunden beeinträchtigt sind;
- das Recht, allgemeine Richtlinien und spezifische Anweisungen an den Dienstleister zu den Aspekten zu erteilen, die bei der Erbringung der Dienstleistungen zu berücksichtigen sind;¹⁵
- das Recht, dass die Aufsichtsbehörde, sofern dies für Aufsichtszwecke angemessen und erforderlich ist, Fragen direkt an den Dienstleister richten kann, die von diesem zu beantworten sind.¹⁶
- die Verpflichtung des Dienstleisters, bei Vor-Ort-Kontrollen und Audits durch die zuständige nationale und europäische Behörde, den Kunden oder einen beauftragten Dritten uneingeschränkt zu kooperieren.
- Der Kunde teilt dem Dienstleister nach Möglichkeit im Voraus die Einzelheiten zum Umfang und zur Häufigkeit der Vor-Ort-Kontrollen sowie zum Ablauf mit. Die Audits können alle Bereiche umfassen, die für die Erbringung der vertraglich vereinbarten Dienstleistungen relevant sind. Bei der Durchführung dieser Audits hält sich der Kunde an die allgemein anerkannten Auditstandards in Übereinstimmung mit den Aufsichts-anweisungen für die Anwendung und Einbeziehung solcher Auditstandards.¹⁷

8.2. Der Dienstleister ist verpflichtet, uneingeschränkt mit den für den Kunden zuständigen Behörden und Abwicklungsbehörden, einschließlich der von ihnen benannten Personen, zusammenzuarbeiten.¹⁸

8.3. Zusätzlich zu den Audits verpflichtet sich der Dienstleister, an den Schwachstellen- oder bedrohungsorientierten Penetrationstests des Kunden teilzunehmen und dabei uneingeschränkt zu kooperieren.¹⁹

8.4. Auf Wunsch des Kunden legt der Dienstleister dem Kunden folgende Berichte vor: regelmäßige Berichte (einschließlich des internen Prüfungsberichts des Dienstleisters) und Berichte über (i) IKT-Vorfälle, (ii) die Erbringung von Dienstleistungen, (iii) IKT-Sicherheit, (iv) Maßnahmen und Tests zur Aufrechterhaltung des Betriebs, (v) Prüfungsberichte der externen Wirtschaftsprüfer des Dienstleisters.²⁰

9 Kündigungsbestimmungen²¹

9.1. Der Kunde ist berechtigt, den Vertrag einschließlich dieser Zusatzvereinbarung oder einzelne, definierbare Teilleistungen aus wichtigem Grund sofort oder zu einem vom Kunden bestimmten Zeitpunkt zu kündigen, insbesondere wenn eines der folgenden Ereignisse eintritt:²²

- Ein wesentlicher Verstoß des Dienstleisters gegen geltende Gesetze, Vorschriften oder die Bestimmungen des Vertrags oder dieser Zusatzvereinbarung;

¹⁵ Siehe Art. 274 Abs. 4 Buchstabe f DelVO 2015/35.

¹⁶ Siehe Art. 274 Abs. 4 Buchstabe i DelVO 2015/35.

¹⁷ Siehe Art. 274 Abs. 4 Buchstabe f DelVO 2015/35.

¹⁸ Dieser Punkt setzt Art. 30 Abs. 2 Buchstabe g der DORA-Verordnung um.

¹⁹ Dieser Punkt setzt Art. 30 Abs. 3 Buchstabe d DORA-Verordnung um.

²⁰ Siehe auch Randnummer 37 Buchstabe j ELOPA-BoS-20-002.

Dieser Punkt setzt unter anderem Art. 8 Abs. 2 Buchstabe d DelVO (EU) 2024/1773 um (RTS zur Festlegung des detaillierten Inhalts der Richtlinie über vertragliche Vereinbarungen zur Nutzung von IKT-Diensten, die kritische oder wichtige Funktionen unterstützen und von externen IKT-Dienstleistern bereitgestellt werden).

²¹ Dieses Kapitel setzt Randnummer 37 Buchstabe b von ELOPA-BoS-20-002, Art. 274 Abs. 4 Buchstabe d DelVO 2015/35 und Art. 30 Abs. 2 Buchstabe h und Art. 28 Abs. 7 DORA-Verordnung um.

²² Dieser Punkt setzt Artikel 28 Absatz 7 der DORA-Verordnung um.

- Es liegen nachweisbare Schwächen im gesamten IKT-Risikomanagement des Dienstleisters vor, insbesondere in der Art und Weise, wie er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder sonstige sensible Daten oder um nicht personenbezogene Daten oder Informationen handelt;
- Eine wirksame Aufsicht über den Kunden durch die Aufsichtsbehörde ist aufgrund der Bestimmungen des Vertrags und dieser Zusatzvereinbarung oder der mit diesen Verträgen verbundenen Umstände nicht mehr möglich;
- Im Rahmen der Überwachung des IKT-Risikos Dritter wurden Umstände festgestellt, die sich wahrscheinlich auf die Erfüllung der in der Vereinbarung und dieser Zusatzvereinbarung vorgesehenen Funktionen auswirken, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder diese Zusatzvereinbarung oder die Situation des Dienstleisters auswirken;
- im Falle des Einsatzes eines Subunternehmers ohne entsprechende Zustimmung des Kunden oder im Falle einer wesentlichen Änderung der Untervergabe ohne entsprechende Zustimmung oder im Falle des Einsatzes eines Subunternehmers über den genehmigten Leistungsumfang hinaus.²³

9.2. Die Parteien vereinbaren, dass sie – unabhängig von der Form der Kündigung und dem Kündigungsgrund – zusammenarbeiten werden, um eine ordnungsgemäße Beendigung und Migration der Dienstleistungen auf den Kunden selbst oder einen von ihm benannten Dritten zu erreichen. Zu diesem Zweck wird der Dienstleister die nachstehend definierten Unterstützungsleistungen für den Übergang („Kündigungsunterstützung“) erbringen und auf Wunsch des Kunden die Erbringung der Dienstleistungen verlängern („Nachwirkung“). Der Kunde hat auch im Falle einer nur teilweisen Kündigung des Vertrags Anspruch auf diese Rechte.

9.3. Die Kündigungsunterstützung des Dienstleisters umfasst die Erbringung aller Unterstützungsleistungen, die eine reibungslose Migration der vom Dienstleister im Rahmen des Vertrags geschuldeten gekündigten Dienste auf den Kunden oder einen vom Kunden benannten Dritten vom Zeitpunkt der Kündigung bis [12] Monate nach dem Wirksamwerden der Kündigung oder nach Ablauf einer vereinbarten Nachwirkung („Unterstützungszeitraum“) ermöglichen. Der Dienstleister erbringt die Kündigungsunterstützungsleistungen auf schriftliche Anfrage des Kunden unter auf der Grundlage der vereinbarten Geschäftsbedingungen. Werden die Unterstützungsleistungen aufgrund einer Kündigung aus wichtigem Grund durch den Kunden erbracht, hat der Dienstleister keinen Anspruch auf eine Vergütung für seine Tätigkeiten zur Minimierung des Schadens des Kunden. Bei der Erbringung der Leistungen hält sich der Dienstleister nach besten Kräften an den Zeitplan des Kunden.

Auf Wunsch des Kunden erbringt der Dienstleister während der Unterstützungsphase alle Dienstleistungen, die für eine reibungslose Migration zum nachfolgenden Auftragnehmer erforderlich oder zweckmäßig sind.

Ist der Kunde oder der nachfolgende Auftragnehmer nach Beendigung des Vertrags nicht in der Lage, die Erbringung der Dienstleistungen zu übernehmen, erbringt der Dienstleister auf schriftliche Anfrage des Kunden alle Dienstleistungen auf der Grundlage des Vertrags für einen Zeitraum von maximal [24] Monaten nach dem wirksamen Ende des Vertrags weiter.

10 Verteilung von Rechten und Pflichten

Eine klare Zuordnung der Rechte und Pflichten zwischen dem Kunden und dem Dienstleister ist schriftlich im Vertrag, einschließlich aller Anhänge, festzuhalten, um den geltenden gesetzlichen und behördlichen Bestimmungen für die gesamte Laufzeit des Vertrags zu entsprechen. ⁱ

11 Ergänzungen

Da im Zusammenhang mit der Umsetzung und Auslegung der DORA-Verordnung noch delegierte Rechtsakte und weitere Konkretisierungen durch die zuständigen europäischen und nationalen Aufsichtsbehörden zu erwarten sind, werden die Vertragsparteien die entsprechenden Anforderungen beobachten und sich gegenseitig entsprechend informieren.

11.1. In diesem Zusammenhang verpflichtet sich der Dienstleister, bei der Ausarbeitung der neuen Fassung oder Änderung dieser Zusatzvereinbarung mitzuwirken, insbesondere durch Bereitstellung der erforderlichen Informationen.

²³ Dieser Punkt setzt Art. 7 Abs. 1 RTS zur Untervergabe um.

- 11.2. Unabhängig davon ist der Dienstleister in jedem Fall verpflichtet, notwendige Änderungen der Anforderungen und Inhalte umzusetzen, soweit diese gesetzlich vorgeschrieben sind. Andernfalls steht dem Kunden ein außerordentliches Kündigungsrecht zu.

12 Geltungsreihenfolge

Die Bestimmungen des Vertrags gelten weiterhin, und diese Zusatzvereinbarung mit ihren Anhängen, die integraler Bestandteil der Zusatzvereinbarung sind, ergänzt lediglich die geltenden Bestimmungen des Vertrags.

Bei Unstimmigkeiten, Unklarheiten oder Widersprüchen zwischen dem Vertrag und dieser Zusatzvereinbarung hat diese Zusatzvereinbarung Vorrang, es sei denn, strengere Bestimmungen des Vertrags beruhen auf gesetzlichen Vorschriften oder behördlichen Auflagen.

ⁱⁱ Dieser Punkt setzt Art. 30 Abs. 2 Buchstabe a der DORA-Verordnung und R 37 Buchstabe a der EIOPA-Leitlinien EIOPA-BoS-20-002 um.