



Investitions- und Strukturbank

Rheinland-Pfalz (ISB)

ZUSATZVERTRAG ZU VERTRÄGEN ÜBER DIE AUSLAGERUNG VON LEISTUNGEN UND/ODER  
VERTRÄGEN ÜBER DIE ERBRINGUNG VON IKT-DIENSTLEISTUNGEN (ZUSATZVERTRAG)

Zusatzvertrag

zwischen

Investitions- und Strukturbank Rheinland-Pfalz (ISB)

Holzhofstr. 4

55116 Mainz

(nachfolgend „Auftraggeber“ genannt)

und

[XXX]

(nachfolgend „Auftragnehmer“ genannt)

Der Auftraggeber und der Auftragnehmer gemeinsam werden nachfolgend auch „Parteien“ oder „Vertragsparteien“ genannt.

<b>1</b>	<b>Präambel.....</b>	<b>4</b>
1.1	Regulatorischer Rahmen .....	4
1.2	Konkreter Anwendungsbereich dieses Zusatzvertrages .....	5
1.3	Änderungen der aufsichtsrechtlichen Anforderungen .....	5
<b>2</b>	<b>Allgemeine Bestimmungen .....</b>	<b>5</b>
2.1	Mitarbeiterqualifikation, Mindestlohn und Erlaubnisse.....	5
2.2	Allgemeine Mitwirkungsleistungen des Auftraggebers .....	6
2.3	Geheimhaltung, Bankgeheimnis .....	6
2.4	Nachhaltigkeit .....	7
2.5	Schriftform, salvatorische Klausel .....	7
2.6	Gerichtsstand, Anwendbares Recht .....	7
<b>3</b>	<b>Mindestinhalte Art. 30 Abs. 2 DORA (Einfache IKT-Leistung).....</b>	<b>8</b>
3.1	Leistungsbeschreibung (Art. 30 Abs. 2 lit. a) DORA).....	8
3.2	Einsatz von Subunternehmern (Art. 30 Abs. 2 lit. a) DORA) .....	8
3.3	Standorte und Datenspeicherorte (Art. 30 Abs. 2 lit. b) DORA) .....	9
3.4	Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten (Art. 30 Abs. 2 lit. c) DORA) .....	9
3.5	Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten (Art. 30 Abs. 2 lit. d) DORA).....	10
3.6	Beschreibungen der Dienstleistungsgüte (Art. 30 Abs. 2 lit. e) DORA) .....	10
3.7	Unterstützung bei IKT-Vorfällen (Art. 30 Abs. 2 lit. f) DORA).....	11
3.8	Zusammenarbeit mit Behörden (Art. 30 Abs. 2 lit. g) DORA).....	11
3.9	Kündigungsrechte (Art. 28 Abs. 7, Art. 30 Abs. 2 lit. h) DORA).....	11
3.10	Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen (Art. 30 Abs. 2 lit. i) DORA).....	11
<b>4</b>	<b>Mindestinhalte Art. 30 Abs. 3 DORA.....</b>	<b>12</b>
4.1	Vollständige Beschreibungen der Dienstleistungsgüte (Art. 30 Abs. 3 lit. a) DORA) .....	12
4.2	Einsatz von Subunternehmern.....	12
4.3	Kündigungsfristen und Berichtspflichten (Art. 30 Abs. 3 lit. b) DORA) .....	13
4.4	Notfallmanagement (Art. 30 Abs. 3 lit. c) DORA) .....	14
4.5	Informationssicherheit (Art. 30 Abs. 3 lit. c) DORA) .....	14

4.6	TLPT des Auftraggebers (Art. 30 Abs. 3 lit. d) DORA).....	14
4.7	Überwachung (Art. 30 Abs. 3 lit. e) DORA) .....	15
4.8	Exit Management (Art. 30 Abs. 3 lit. f) DORA) .....	15
<b>5</b>	<b>Auslagerungsanforderungen (§ 25 b KWG, AT 9 Tz. 7 MaRisk).....</b>	<b>16</b>
5.1	Vertragsgegenstand und Dienstleistungsgüter (AT 9 Tz. 7 lit. a) und lit. e) MaRisk).....	16
5.2	Vertragsbeginn, Dauer, (AT 9 Tz. 7 lit. b) MaRisk) .....	16
5.3	Standorte (AT 9 Tz. 7 lit. d) MaRisk) .....	16
5.4	Versicherung (AT 9 Tz. 7 lit. f) MaRisk) .....	16
5.5	Notfallmanagementkonzept (AT 9 Tz. 7 lit. g) MaRisk) .....	16
5.6	Koordination, Berichtspflichten und laufende Kontrolle (AT 9 Tz. 7 lit. h MaRisk).....	16
5.7	Interne Revision, Externe Wirtschaftsprüfer, Prüfungsrechte zuständiger Aufsichts-behörden (AT 9 Tz. 7 lit. h), i) MaRisk) .....	17
5.8	Weisungen (AT 9 Tz. 7 lit. j) MaRisk) .....	18
5.9	Datenschutz (AT 9 Tz. 7 lit. k) MaRisk) .....	18
5.10	Sicherheits- und Risikomanagement (AT 9 Tz. 7 lit. k) MaRisk) .....	18
5.11	Kündigung (AT 9 Tz. 7 lit. l) MaRisk).....	19
5.12	Exit Management .....	20
5.13	Weiterverlagerung (AT 9 Tz. 7 lit. m MaRisk) .....	20
5.14	Informationspflichten (AT 9 Tz. 7 lit. n MaRisk).....	22
<b>6</b>	<b>ANLAGEN .....</b>	<b>23</b>

# **1 Präambel**

## **1.1 Regulatorischer Rahmen**

- 1.1.1 Der Auftraggeber unterliegt als Kreditinstitut insbesondere der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor („DORA“) und den aufsichtsrechtlichen Anforderungen nach §§ 25a, § 25b KWG sowie die Mindestanforderungen an das Risikomanagement der Kreditinstitute (MaRisk). Dieser Zusatzvertrag setzt die Anforderungen gemäß DORA und MaRisk um und ergänzt den Vertrag vom [TT.MM.JJJJ] über [Name des Hauptvertrages] (nachfolgend „Vertrag“ genannt)
- 1.1.2 Sofern die unter dem Vertrag durch den Auftragnehmer bereitgestellten Vertragsleistungen IKT-Dienstleistungen im Sinne von Art. 3 Nr. 21 DORA sind, gelten gemäß Kapitel 1.2 die Regelungen zur Umsetzung der Mindestvertragsinhalte des Art. 30 DORA:
- a) Bestimmungen gemäß Kapitel 3: Vertragsleistungen, die nur IKT-Dienstleistungen umfassen, die nicht der Unterstützung kritischer oder wichtiger Funktionen gemäß Art. 3 Nr. 22 DORA dienen („einfache IKT-Dienstleistungen“)
  - b) Bestimmungen der Kapitel 4: Vertragsleistungen, die auch IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß Art. 3 Nr. 22 DORA umfassen.
- 1.1.3 Dieser Zusatzvertrag erfüllt mit den Bestimmungen in Kapitel 5 die aufsichtsrechtlichen Anforderungen nach §§ 25a, § 25b KWG sowie die Mindestanforderungen an das Risikomanagement der Kreditinstitute (MaRisk), insb. AT 9. Der Auftragnehmer ist verpflichtet, die Vertragsleistungen für den Auftraggeber nach den Regeln banküblicher Sorgfalt zu erbringen.
- 1.1.4 Der Auftragnehmer wird insbesondere die für den Auftraggeber und seine Leistungserbringung geltenden IT-sicherheitstechnischen und revisionsrelevanten Bestimmungen sowie die im Folgenden vereinbarten Qualitäts- und Leistungsstandards einhalten. Der Auftragnehmer hat sich über die Fortschreibung der für die Durchführung der Vertragsleistung geltenden gesetzlichen Bestimmungen selbstständig zu informieren und für deren Umsetzung Sorge zu tragen. Darüberhinausgehende institutsspezifische Bestimmungen hat der Auftraggeber dem Auftragnehmer entsprechend mitzuteilen, so dass dieses der Umsetzung nachkommen kann. Für die Durchführung der Vertragsleistung sind insbesondere verbindlich:
- a) die jeweils für die Rechnungslegung, Buchführung und Geschäftsabwicklung in den Kreditinstituten geltenden Rechtsvorschriften, insbesondere handels-, steuer- und aufsichtsrechtliche Vorschriften,
  - b) die Anforderungen an eine ordnungsgemäße und sichere Datenverarbeitung sowie an den Datenschutz,
  - c) und folgende fachliche und prüferische Standards:
    - die Rechnungslegungs- und Prüfungsstandards des Auftraggebers (IDW PS 951, ISAE 3402, etc.).

## **1.2 Konkreter Anwendungsbereich dieses Zusatzvertrages**

Für den zwischen den Vertragsparteien geschlossenen Vertrag gelten folgende Bestimmungen (jeweils einschließlich der kapitelübergreifenden Verweisungen):

- ☒ Bestimmungen für einfache IKT-Leistungen gemäß Kapitel 3.
- ☐ Bestimmungen für IKT-Leistungen zur Unterstützung einer kritischen/wichtigen Funktion gemäß Kapitel 4 gelten zusätzlich zu den Anforderungen in Kapitel 3. Der Auftraggeber teilt dem Auftragnehmer die jeweilige Einstufung einer IKT-Dienstleistung als zur Unterstützung kritischer oder wichtiger Funktionen mit und kann diese Einstufung jederzeit durch schriftliche Mitteilung an den Auftragnehmer (E-Mail ausreichend) ändern.
- ☒ Bestimmungen für alle Auslagerungen gemäß Kapitel 5.

## **1.3 Änderungen der aufsichtsrechtlichen Anforderungen**

- 1.3.1 Bei einer wesentlichen Änderung des regulatorischen Rahmens gemäß Kapitel 1.1 einschließlich der maßgeblichen Leistungs- und Qualitätsstandards, durch die die Geschäfts- bzw. Kalkulationsgrundlage des Vertrages nicht mehr gegeben ist und/oder von Behörden ggü. dem Auftraggeber angeordneten Änderungen am Vertrag, verpflichten sich die Parteien, schriftlich eine angepasste oder, sofern dies nicht möglich ist, neue Vereinbarung zu treffen, die der Zielsetzung dieses Zusatzvertrages unter Berücksichtigung der neuen Vorgaben am nächsten kommt.
- 1.3.2 Wird ein schriftlicher Änderungsantrag eingereicht, so wird die jeweilige Empfangspartei diesen auf eigene Kosten innerhalb von 15 Arbeitstagen nach Zugang des Änderungsantrages prüfen und entscheiden, sofern der Änderungsantrag nicht ausdrücklich eine längere Frist setzt. Die Annahme des Antrags durch die Empfangspartei hat schriftlich unter Bezugnahme auf den Änderungsantrag sowie den vorliegenden Vertrag zu erfolgen. Die Ablehnung des Antrags darf nur erfolgen, wenn die Änderungen für die Empfangspartei unzumutbar sind. Sie hat ebenfalls schriftlich unter Bezugnahme auf den Änderungsantrag sowie den vorliegenden Vertrag unter Darlegung der zur Ablehnung führenden Gründe zu erfolgen. Bei Weigerung zur Umsetzung seitens des Auftragnehmers hat der Auftraggeber ein außerordentliches, sofortiges Sonderkündigungsrecht hinsichtlich aller nicht mehr den aufsichtsrechtlichen oder den sonstigen rechtlichen Vorgaben entsprechenden Vertragsleistungen.
- 1.3.3 Die Änderung oder Einführung von Servicestandards kann von dem Auftraggeber einseitig nach billigem Ermessen bestimmt werden, vgl. § 315 BGB. Der Auftraggeber hat den Auftragnehmer über Änderungen zu informieren und diese zu dokumentieren. Sollte die Anpassung kosten- oder budgetrelevant sein, erfolgt eine Überprüfung und ggf. Anpassung der Verrechnungspreise.

## **2 Allgemeine Bestimmungen**

### **2.1 Mitarbeiterqualifikation, Mindestlohn und Erlaubnisse**

- 2.1.1 Der Auftragnehmer verpflichtet sich sicherzustellen, dass für die Vertragsleistungen geeignetes, zuverlässiges und ausreichend fachlich qualifiziertes Personal eingesetzt wird. Soweit zur Erbringung der Vertragsleistungen erforderlich oder gesetzlich vorgeschrieben, wird der Auftragnehmer sein Personal entsprechend schulen. Auf Verlangen des Auftraggebers wird der

Auftragnehmer die Erfüllung der vorgenannten Verpflichtungen auf geeignete Art und Weise nachweisen.

- 2.1.2 Der Auftragnehmer verpflichtet sich zur Zahlung des gesetzlichen Mindestlohnes. In gleicher Weise verpflichtet sich der Auftragnehmer die von ihm beauftragten Subunternehmer auf die Zahlung des Mindestlohnes zu verpflichten.
- 2.1.3 Der Auftragnehmer versichert, dass es über die für seine Tätigkeit gegebenenfalls erforderlichen Erlaubnisse, Zulassungen und/oder Registrierungen verfügt und verpflichtet sich, diese während der Vertragslaufzeit aufrecht zu erhalten. Auf Verlangen des Auftraggebers wird der Auftragnehmer die Erfüllung der vorgenannten Verpflichtungen auf geeignete Art und Weise nachweisen.

## **2.2 Allgemeine Mitwirkungsleistungen des Auftraggebers**

- 2.2.1 Der Auftraggeber schafft in seinem Verantwortungsbereich auf seine Kosten die für die Erbringung der Vertragsleistungen notwendigen Voraussetzungen und Mitwirkungsleistungen so rechtzeitig, dass dem Auftragnehmer für die Erfüllung seiner Pflichten eine angemessene Vorlaufzeit verbleibt. Die jeweiligen Pflichten der Parteien ergeben sich aus den Regelungen dieser Zusatzvereinbarung (siehe Kapiteln 3.1, 4.1, 5.1).
- 2.2.2 Der Auftraggeber wird der Auftragnehmer über für die Erbringung der Vertragsleistungen relevante technische und organisatorische Veränderungen in seinem Geschäftsbetrieb (z. B. durch Fusion, Zukäufe, Umstrukturierung, Übernahme anderer Kreditinstitute bzw. Unternehmen), Planungen bezüglich Änderungen seines Geschäftsvolumens und seines Geschäftsmodells sowie der Aufnahme von Geschäftsaktivitäten in Gestalt neuer Produkte oder auf neuen Märkten rechtzeitig unterrichten, damit der Auftragnehmer die Erbringung seiner Vertragsleistung darauf abstimmen kann.
- 2.2.3 Leistungsspezifische Mitwirkungsleistungen, Beistellungsleistungen sowie gegebenenfalls erforderliche Vollmachten werden von den Parteien gesondert festgelegt.

## **2.3 Geheimhaltung, Bankgeheimnis**

- 2.3.1 Die Parteien sind verpflichtet, sämtliche ihnen im Zusammenhang mit dem Vertrag zugänglich werdenden Informationen unbefristet geheim zu halten, soweit diese dem Geschäftsgeheimnisgesetz, dem Bankgeheimnis oder dem Datengeheimnis nach den geltenden Datenschutzgesetzen unterfallen oder interne Geschäftsabläufe des jeweiligen Vertragspartners oder Kundendaten des Auftraggebers betreffen und/oder nicht öffentlich bekannt sind. Die Parteien werden ihre Mitarbeiter und Dritte, durch die sie ggf. Aufträge ausführen lassen, Kenntnis nur bei Bedarf verschaffen und schriftlich zur Geheimhaltung und zur Wahrung des Datengeheimnisses nach den geltenden Datenschutzgesetzen sowie des Bankgeheimnisses verpflichten. Beauftragte Dritte sind zu verpflichten, ihrerseits ihre Mitarbeiter durch geeignete Vereinbarungen entsprechend zu verpflichten.
- 2.3.2 Insbesondere wird der Auftragnehmer alle in seinen Besitz gelangten Informationen, Dateien und Unterlagen des Auftraggebers sorgfältig verwahren und vor Einsichtnahme Unbefugter schützen sowie alle erforderlichen organisatorischen Maßnahmen treffen, Kundendaten vor unbefugtem Zugang zu schützen. Es wird die Unterlagen, die Informationen im Sinne von Kapitel 2.3.1 enthalten, sowie Vervielfältigungen irgendwelcher Art hiervon an den Auftraggeber herausgeben, sobald es diese zur Erfüllung seiner vertraglichen Pflichten nicht mehr

benötigt. Ein Zurückbehaltungsrecht, gleich aus welchem Rechtsgrund, kann insoweit nicht geltend gemacht werden.

- 2.3.3 Der Auftragnehmer hat durch besondere technische, personelle und organisatorische Maßnahmen sicherzustellen, dass im Fall der Erbringung von Leistungen für mehrere auslagernde Institute die Vertraulichkeit der Daten zwischen den verschiedenen auslagernden Instituten gewahrt bleibt.

## **2.4 Nachhaltigkeit**

- 2.4.1 Der Auftraggeber hat das Thema Nachhaltigkeit in sein Geschäftsmodell integriert und beachtet im Rahmen seiner Geschäftstätigkeiten gesellschaftliche, ökologische, ethische und soziale Aspekte entlang der gesamten Wertschöpfungskette. Nachhaltigkeit spielt für den Auftragnehmer eine wichtige Rolle. Für den Auftraggeber bedeutet Nachhaltigkeit, dass der wirtschaftliche Erfolg mit sozialer und ökologischer Verantwortung im Einklang steht. Der Auftragnehmer handelt verantwortungsvoll gegenüber Kunden, Beschäftigten, Lieferanten und Kooperationspartnern.
- 2.4.2 Der Auftragnehmer verpflichtet sich die vorgesehenen Unternehmenswerte und den Verhaltenskodex des Auftraggebers einzuhalten. Des Weiteren verpflichtet sich der Auftragnehmer, die Regelungen der **Anlage 1** (Nachhaltigkeitsanforderungen und Unternehmenswerte) einzuhalten.

## **2.5 Schriftform, salvatorische Klausel**

- 2.5.1 Änderungen und Ergänzungen dieses Zusatzvertrages und/oder die anderweitige Abgabe von Willenserklärungen bedürfen der Schriftform gemäß § 126 BGB oder der elektronischen Form des § 126a BGB. Das gilt auch für Abweichungen vom Formerfordernis.
- 2.5.2 Sollten einzelne oder mehrere Bestimmungen dieses Zusatzvertrages ganz oder teilweise unwirksam sein, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, unwirksame Bestimmungen durch Regelungen zu ersetzen, die dem Gewollten wirtschaftlich möglichst nahekommen.

## **2.6 Gerichtsstand, Anwendbares Recht**

- 2.6.1 Der Vertrag und dieser Zusatzvertrag unterliegen deutschem Recht.
- 2.6.2 Gerichtsstand ist Mainz.

### **3 Mindestinhalte Art. 30 Abs. 2 DORA (Einfache IKT-Leistung)**

#### **3.1 Leistungsbeschreibung (Art. 30 Abs. 2 lit. a) DORA)**

- 3.1.1 Die Rechte und Pflichten der Parteien im Hinblick auf die Vertragsleistungen werden im Vertrag eindeutig zugewiesen und schriftlich dargelegt.
- 3.1.2 Der Auftragnehmer erbringt die Vertragsleistungen wie im Vertrag und dessen sämtlichen Anlagen und sonstigen Anhängen, insbesondere in der jeweiligen Leistungsbeschreibung, Funktions- oder Produktbeschreibung näher beschrieben.

#### **3.2 Einsatz von Subunternehmern (Art. 30 Abs. 2 lit. a) DORA)**

- 3.2.1 Der Auftragnehmer ist berechtigt, mit der Erbringung der Vertragsleistungen einen Dritten (im Folgenden „Subunternehmer“) zu beauftragen, sofern dies nach geltendem Recht zulässig ist und dieser die erforderliche Zuverlässigkeit und fachliche Eignung besitzt. Der Auftragnehmer ist verpflichtet, den Auftraggeber rechtzeitig vor einem geplanten Subunternehmereinsatz zu informieren. Der Auftragnehmer hat dem Auftraggeber im Zusammenhang dem geplanten Subunternehmereinsatz auf Verlangen des Auftraggebers, sämtliche Unterlagen und Informationen zur Verfügung zu stellen, die der Auftraggeber für eine Risikoanalyse, Risikobewertung und Wesentlichkeitseinstufung benötigt.
- 3.2.2 Der Auftragnehmer darf Subunternehmer nur mit der Erbringung von nach dem Vertrag geschuldeten Vertragsleistungen beauftragen, wenn der Auftraggeber dem Einsatz nicht binnen einer Frist von acht (8) Wochen aus wichtigem Grund widerspricht. Ein wichtiger Grund ist insbesondere dann gegeben, wenn sich das Risikoprofil der Vertragsleistung verändert oder dem Auftraggeber zusätzliche Kosten und/oder anderweitigen rechtliche oder wirtschaftliche Nachteile entstehen. Für den Einsatz neuer Subunternehmer und wesentlicher Änderungen bestehender Unterauftragsverhältnisse gilt Kapitel 3.2.2 entsprechend. Sofern der Vertrag einen Zustimmungsvorbehalt für den Einsatz von Subunternehmern vorsieht, haben die Bestimmungen des Vertrags Vorrang vor diesem Kapitel 3.2.2.
- 3.2.3 Der Auftragnehmer verpflichtet sich, seine vertraglichen Vereinbarungen mit den Subunternehmern in Schriftform oder in einem anderen herunterladbaren, dauerhaften und zugänglichen Format und nur im Einklang mit den Regelungen des Vertrages und dieses

Zusatzvertrages auszugestalten. Der Auftragnehmer muss in seiner vertraglichen Vereinbarung mit dem jeweiligen Subunternehmer

- 3.2.3.1 die Überwachungs- und Berichtspflichten, die der Subunternehmer gegenüber dem Auftragnehmer und dem Auftraggeber entsprechend dem Vertrag und diesem Zusatzvertrag erfüllen muss, festlegen;
- 3.2.3.2 den Subunternehmer zur Umsetzung von Notfallplänen und die vom Subunternehmer einzuhaltende Service Levels festlegen;
- 3.2.3.3 den Subunternehmer zur Einhaltung der im Vertrag und diesem Zusatzvertrag vereinbarten IT-Sicherheitsstandards und zusätzlicher angemessener Sicherheitsstandards, soweit notwendig, verpflichten; und
- 3.2.3.4 den Subunternehmer verpflichten, dass der Subunternehmer dem Auftraggeber und den zuständigen Aufsichtsbehörden mindestens die gleichen Prüfungs-, Informations- und Zugangsrechte gewährt, wie diese im Vertrag und diesem Zusatzvertrag vorgesehen sind.
- 3.2.4 Die Subunternehmer erbringen ihre Leistungen, einschließlich der Verarbeitung und Speicherung von Daten, ausschließlich an den gemäß Kapitel 3.3 festgelegten Leistungsstandorten.
- 3.2.5 Der Auftragnehmer wird dem Auftraggeber die Einhaltung dieser Kapitel 3.2 auf Verlangen in geeigneter Form nachweisen.

### **3.3 Standorte und Datenspeicherorte (Art. 30 Abs. 2 lit. b) DORA)**

- 3.3.1 Der bzw. die Standort(e), an denen die Vertragsleistungen vom Auftragnehmer erbracht und/oder Daten gespeichert und verarbeitet werden, entsprechen dem im Vertrag angegebenen Sitz des Auftragnehmers.
- 3.3.2 Wenn Standorte, einzelne Vertragsleistungen oder die gesamte Vertragsleistung innerhalb des EWR verlagert werden sollen, erfordert dies die Zustimmung des Auftraggebers. Der Auftraggeber wird seine Zustimmung zur Verlagerung des Standorts nur aus wichtigem Grund verweigern. Ein wichtiger Grund ist insbesondere dann gegeben, wenn sich das Risikoprofil der Vertragsleistung verändert oder dem Auftraggeber zusätzliche Kosten und/oder anderweitigen rechtliche oder wirtschaftliche Nachteile entstehen.
- 3.3.3 Die Zustimmung zu Standortverlagerung(en) außerhalb des EWR liegt im freien Ermessen des Auftraggebers. Darüber hinaus verpflichtet sich der Auftragnehmer in diesem Fall zur Benennung eines inländischen Zustellungsbevollmächtigten, an den Bekanntgaben und Zustellungen durch die BaFin oder andere Aufsichtsbehörden bewirkt werden können.

### **3.4 Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten (Art. 30 Abs. 2 lit. c) DORA)**

- 3.4.1 Der Auftragnehmer trägt dafür Sorge, dass alle datenschutzrechtlichen Bestimmungen eingehalten werden. Der Auftragnehmer hat für die Vertraulichkeit und die Richtigkeit sämtlicher Kunden-Daten (einschließlich personenbezogener Daten) zu sorgen und implementiert angemessene technische und organisatorische Maßnahmen zur Sicherstellung von Verfügbarkeit,

Integrität und Vertraulichkeit sämtlicher Kunden-Daten. Die Strafbarkeit einer Verletzung des Datengeheimnisses ist ihm bekannt.

- 3.4.2 Im Rahmen der Leistungserbringung kommt der Auftragnehmer potenziell mit personenbezogenen Daten des Auftraggebers in Berührung, die der Auftraggeber als Verantwortlicher im Sinne von Artikel 4 Nr. 7 DSGVO verarbeitet. Zur Regelung des Auftragsverarbeitungsverhältnisses gilt der Auftragsverarbeitungsvertrag in **Anlage 2**.

- 3.4.3 Der Auftraggeber unterfällt dem Landesdatenschutzgesetz Rheinland-Pfalz. Der Auftraggeber kann daher gegenüber dem Auftragnehmer zusätzliche Anforderungen zum Datenschutz stellen, soweit diese sich zwingend aus dem Landesdatenschutzgesetz Rheinland-Pfalz ergeben und über die Anforderungen des BDSG sowie der DSGVO hinausgehen. Der Auftragnehmer wird diese Anforderungen prüfen und - soweit erforderlich und wirtschaftlich angemessenen - sich mit dem Auftraggeber über eine Umsetzung abstimmen. Der Auftraggeber wird dem Auftragnehmer einen eventuellen Mehraufwand vergüten.

### **3.5 Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten (Art. 30 Abs. 2 lit. d) DORA)**

- 3.5.1 Der Auftragnehmer gewährleistet den Zugang zu allen personenbezogenen und nicht personenbezogenen Daten, die im Rahmen der Vertragsleistungen verarbeitet werden, insbesondere im Fall einer Insolvenz, Abwicklung, oder Einstellung der Geschäftstätigkeit des Auftragnehmers oder einer Beendigung des Vertrages, sowie die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format.
- 3.5.2 Der Auftragnehmer ist insbesondere verpflichtet, für eine insolvenz sichere Datenhaltung zu sorgen.

### **3.6 Beschreibungen der Dienstleistungsgüte (Art. 30 Abs. 2 lit. e) DORA)**

- 3.6.1 Soweit im Vertrag keine besondere Dienstleistungsgüte festgelegt ist, wird der Auftragnehmer zumindest die Qualität sicherstellen, die von einem professionellen IKT-Drittdienstleister im Finanzdienstleistungssektor im Zusammenhang mit den Vertragsleistungen erwartet werden kann.
- 3.6.2 Stellt der Auftraggeber fest, dass die vereinbarten Service Levels nicht eingehalten werden, kann er den Auftragnehmer jederzeit auffordern, unverzüglich angemessene Korrekturmaß-

nahmen umzusetzen. Der Auftragnehmer wird die Einhaltung der Service Levels kontinuierlich messen und dem Auftraggeber berichten.

### **3.7 Unterstützung bei IKT-Vorfällen (Art. 30 Abs. 2 lit. f) DORA)**

- 3.7.1 Der Auftragnehmer hat unverzüglich, spätestens nach 24 Stunden, bei Feststellen von Vorfällen bei sich oder bei Bekanntwerden von Vorfällen bei seinen Unterauftragnehmern, den Auftraggeber über den Vorfall und den Stand der Bearbeitung des Vorfalls zu informieren.
- 3.7.2 Der Auftragnehmer wird den Auftraggeber bei einem IKT-bezogenen Vorfall gem. Art. 3 Nr. 8 DORA, der mit den Vertragsleistungen in Verbindung steht, ohne zusätzliche Kosten angemessen unterstützen.

### **3.8 Zusammenarbeit mit Behörden (Art. 30 Abs. 2 lit. g) DORA)**

- 3.8.1 Der Auftragnehmer wird vollumfänglich mit den für den Auftraggeber zuständigen Abwicklungsbehörden und sonstigen Behörden (zusammen die „Aufsichtsbehörden“), einschließlich der von diesen benannten Personen, zusammenarbeiten.

### **3.9 Kündigungsrechte (Art. 28 Abs. 7, Art. 30 Abs. 2 lit. h) DORA)**

Ergänzend zu den im Vertrag vereinbarten Kündigungsrechten und -fristen kann der Auftraggeber den Vertrag ohne Einhaltung einer Frist kündigen, wenn

- 3.9.1 ein erheblicher Verstoß des Auftragnehmers gegen geltende Gesetze, sonstige Vorschriften oder Vertragsabreden vorliegt;
- 3.9.2 Umstände vorliegen, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und diese als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen des Vertrages vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf diesen Vertrag oder die Verhältnisse des Auftragnehmers auswirken;
- 3.9.3 nachweisliche Schwächen des Auftragnehmers in Bezug auf sein allgemeines IKT-Risikomanagement vorliegen, insbesondere bei der Art und Weise, in der der Auftragnehmer 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;
- 3.9.4 die Aufsichtsbehörde den Auftraggeber infolge der Vereinbarungen des Vertrages oder der mit dem Vertrag verbundenen Umstände nicht mehr wirksam beaufsichtigen kann.

### **3.10 Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen (Art. 30 Abs. 2 lit. i) DORA)**

- 3.10.1 Der Auftragnehmer führt für seine Mitarbeiter ein kontinuierliches und angemessenes Sensibilisierungs- und Schulungsprogramm für Informationssicherheit durch.
- 3.10.2 Der Auftragnehmer wird auf Verlangen des Auftraggebers an den vom Auftraggeber angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz gemäß Art. 13 Abs. 6 DORA in angemessenem Umfang teilnehmen.

## **4 Mindestinhalte Art. 30 Abs. 3 DORA**

### **4.1 Vollständige Beschreibungen der Dienstleistungsgüte (Art. 30 Abs. 3 lit. a) DORA)**

Es gelten die Bestimmungen in Kapitel 3.1 dieser Zusatzvereinbarung.

### **4.2 Einsatz von Subunternehmern**

In Ergänzung zu den Bestimmungen gemäß Kapitel 3.2 gelten folgende Bestimmungen:

- 4.2.1 Der Auftragnehmer wird den Auftraggeber über alle im Rahmen der Unterauftragnehmer-Kette eingesetzten Subunternehmer vor deren Einsatz informieren und dem Auftraggeber eine Dokumentation der gesamten Subunternehmerkette (inkl. der für das Informationsregister gem. Art. 28 Abs. 3 und 9 DORA relevanten Informationen) in Textform zur Verfügung stellen. Der Auftragnehmer wird die Dokumentation der Subunternehmerkette jeweils aktuell halten und alle Änderungen der Subunternehmerverhältnisse entsprechend dokumentieren. Dem Auftraggeber ist jeweils die aktuelle Fassung der Dokumentation zur Verfügung zu stellen.
- 4.2.2 Der Auftragnehmer wird vor dem Einsatz eines Subunternehmers alle Risiken, einschließlich der IKT-Risiken, die mit den Standorten der eingesetzten oder potenziellen Subunternehmer und ihrer Muttergesellschaft sowie den Standort, von dem aus die Vertragsleistungen erbracht werden, verbunden sind, bewerten und im Rahmen der Ausgestaltung des Einsatzes berücksichtigen. Der Auftragnehmer wird dem Auftraggeber das Ergebnis einer solchen Prüfung auf Verlangen zur Verfügung stellen.
- 4.2.3 Der Auftragnehmer wird dem Auftraggeber jederzeit auf Verlangen bei der Durchführung seiner eigenen Risikobewertungen hinsichtlich des Einsatzes der Subunternehmer im Rahmen der Erbringung der Vertragsleistungen und der Überwachung der gesamten IKT-Subunternehmerkette angemessen unterstützen. Der Auftragnehmer wird dem Auftraggeber auf Verlangen insbesondere alle Informationen und Dokumentationen über den jeweiligen Subunternehmer und das Unterauftragsverhältnis (einschließlich der Vertragsbedingungen zwischen dem Auftragnehmer und dem Subunternehmer, Informationen zu möglichen IKT-Risiken und Informationen zum Erfüllungsgrad relevanter Leistungsindikatoren (KPIs, Service Level)) zur Verfügung stellen, damit der Auftraggeber sich ein umfassendes Bild vom Risiko des Einsatzes des jeweiligen Subunternehmers machen und den Einsatz der Subunternehmer angemessen überwachen kann.
- 4.2.4 Der Auftragnehmer bleibt für die Erfüllung der auf die Subunternehmer übertragenen Vertragsleistungen in dem gleichen Umfang verantwortlich, als würden diese durch den Auftragnehmer selbst erbracht. Der Auftragnehmer ist verpflichtet, die Kontinuität der Erbringung der Vertragsleistungen über die ganze Subunternehmerkette hinweg zu gewährleisten, auch wenn ein Unterauftragnehmer seine vertraglichen Verpflichtungen nicht einhält.
- 4.2.5 Der Auftragnehmer ist verpflichtet, alle untervergebenen Vertragsleistungen zu überwachen, um sicherzustellen, dass seine vertraglichen Verpflichtungen gegenüber dem Auftraggeber kontinuierlich erfüllt werden. Der Auftragnehmer wird den Auftraggeber unverzüglich über alle Entwicklungen unterrichten, die sich wesentlich auf die Risikobewertung hinsichtlich des Einsatzes des jeweiligen Subunternehmers oder die Erbringung der IKT-Leistungen auswirken.

können, insbesondere wenn Anzeichen dafür vorliegen, dass der Auftragnehmer seine vertraglichen Verpflichtungen gegenüber dem Auftraggeber nicht mehr erfüllen kann.

4.2.6 Für den Einsatz neuer Subunternehmer oder wesentlichen Änderungen bestehender Unterauftragsverhältnisse (zusammen „Subunternehmer-Änderungen“) gilt Folgendes:

4.2.6.1 Der Auftragnehmer wird den Auftraggeber mit einer Vorlaufzeit von 3 Monaten („Prüfungsfrist“) über eine geplante Subunternehmer-Änderung informieren. Der Auftragnehmer wird den Auftraggeber bei der Bewertung der Auswirkungen und Risiken der Subunternehmer-Änderung im Rahmen der Prüfungsfrist angemessen unterstützen. Kapitel 4.2.2 gilt entsprechend.

4.2.6.2 Soweit der Auftraggeber einer Subunternehmer-Änderung nicht spätestens zum Ende der Prüfungsfrist widerspricht, ist der Auftragnehmer berechtigt, die Subunternehmer-Änderung umzusetzen. Dies gilt nicht, wenn der Vertrag für den Einsatz von Unterauftragnehmern eine ausdrückliche Zustimmung oder Genehmigung des Auftraggebers vorsieht. In diesem Fall darf der Auftragnehmer die Unterauftragnehmer-Änderung erst umsetzen, wenn der Auftraggeber dieser ausdrücklich zugestimmt hat.

4.2.6.3 Soweit der Auftraggeber innerhalb der Prüfungsfrist im eigenen Ermessen feststellt, dass die Subunternehmer-Änderung die Risikotoleranz des Auftraggebers übersteigt, wird der Auftraggeber vor Ablauf der Prüfungsfrist (i) den Auftragnehmer über das Ergebnis seiner Prüfung informieren, (ii) gegenüber dem Auftragnehmer Widerspruch gegen die Subunternehmer-Änderung einlegen, sowie (iii) den Auftragnehmer über die für die Umsetzung der Subunternehmer-Änderungen notwendigen Modifikationen informieren. Setzt der Auftragnehmer die Subunternehmer-Änderung trotz Widerspruch und ohne die vom Auftraggeber aufgezeigten Modifikationen um, steht es dem Auftraggeber frei, den Vertrag gem. Kapitel 3.9 zu kündigen. Eine etwaige vertragliche Genehmigungsfrist von Unterauftragnehmer-Änderungen bleibt hiervon unberührt.

#### **4.3 Kündigungsfristen und Berichtspflichten (Art. 30 Abs. 3 lit. b) DORA)**

Zusätzlich zu den im Vertrag und dieser Zusatzvereinbarung, insbesondere unter Kapitel 3.9, vereinbarten Kündigungsrechten, kann der Auftraggeber den Vertrag ohne Einhaltung einer Frist auch kündigen, wenn

4.3.1 der Auftragnehmer trotz eines Widerspruchs des Auftraggebers innerhalb der Prüfungsfrist und ohne Implementierung der durch den Auftraggeber geforderten Modifikationen eine Unterauftragnehmer-Änderung umsetzt;

4.3.2 der Auftragnehmer vor Ablauf der Prüfungsfrist eine Unterauftragnehmer-Änderung umsetzt, ohne dass diese vom Auftraggeber ausdrücklich genehmigt wurde;

4.3.3 der Auftragnehmer ohne ausdrückliche Zustimmung des Auftraggebers Vertragsleistungen an Unterauftragnehmer weiterverlagert, wenn für die entsprechende Unterauftragsvergabe ein Zustimmungserfordernis vereinbart wurde; oder

4.3.4 der Auftragnehmer Vertragsleistungen an Unterauftragnehmer weiterverlagert, die ausdrücklich nicht an Unterauftragnehmer vergeben werden dürfen.

#### **4.4 Notfallmanagement (Art. 30 Abs. 3 lit. c) DORA)**

4.4.1 Der Auftragnehmer ist verpflichtet, über ein Notfallmanagementkonzept zu verfügen. Dieses umfasst definierte Notfallszenarien, Geschäftsfortführungs- sowie Wiederherstellungspläne. Das Notfallmanagementkonzept gewährleistet, dass im Notfall, d.h. nach einem Ereignis höherer Gewalt oder einem sonstigen zu einer Betriebsunterbrechung führenden Ereignis, zeitnah Ersatzlösungen zur Verfügung stehen und eine Rückkehr zum Normalbetrieb innerhalb eines angemessenen Zeitraums vorgenommen werden kann. Der Auftragnehmer ist hinsichtlich seines Notfallmanagementkonzeptes verpflichtet,

- a) die ihm übertragenen Tätigkeiten in sein Notfallmanagementkonzept einzubeziehen,
- b) soweit erforderlich dieses an die Erfordernisse des Auftraggebers anzupassen,
- c) die Wirksamkeit und Angemessenheit des Notfallkonzepts durch Notfalltests regelmäßig zu überprüfen und zu testen, auf Verlangen des Auftraggebers gemeinsame Notfallübungen vorzunehmen und
- d) das Notfallkonzept im Notfall entsprechend den dort aufgeführten Vorgaben und praktischen Erfahrungen anzuwenden.

4.4.2 Das Notfallmanagementkonzept sowie dessen wesentliche Änderungen sind dem Auftraggeber zur Kenntnis zu geben. Sofern der Auftraggeber eine Abstimmung seiner Notfallkonzepte mit den Notfallkonzepten des Auftragnehmers für sinnvoll erachtet, kann der Auftraggeber dies verlangen. Sofern vorhanden, wird der Auftragnehmer bezüglich des Notfallkonzepts erstellte Prüfberichte Dritter dem Auftraggeber unverzüglich zur Verfügung stellen.

#### **4.5 Informationssicherheit (Art. 30 Abs. 3 lit. c) DORA)**

Der Auftragnehmer...

- 4.5.1 richtet angemessene Verfahren ein, um die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der Daten mit Relevanz für die ISB sicherzustellen.
- 4.5.2 informiert sich laufend über Bedrohungen und Schwachstellen der IT-Systeme mit Relevanz für die ISB, prüft ihre Relevanz, bewertet ihre Auswirkungen und ergreift, sofern erforderlich, geeignete technische und organisatorische Maßnahmen.
- 4.5.3 richtet die Funktion des Informationssicherheitsbeauftragten ein, der Vorgaben zur Informationssicherheit in Anlehnung an einen gängigen Standard (z.B. ISO/IEC 2700x oder BSI Grundschutz-Kompendium) definiert sowie deren Einhaltung regelmäßig sowie anlassbezogen überprüft und überwacht.
- 4.5.4 richtet angemessene Verfahren ein, um bei einem Informationssicherheitsvorfall die potenziellen Auswirkungen auf die ISB zeitnah zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen.

#### **4.6 TLPT des Auftraggebers (Art. 30 Abs. 3 lit. d) DORA)**

4.6.1 Soweit der Auftraggeber gemäß Art. 26 und 27 DORA zur Durchführung von TLTP Penetrationstests verpflichtet ist, hat der Auftraggeber das Recht, solche TLTP Penetrationstests zur

Überprüfung der durch den Auftragnehmer umgesetzten IT-Sicherheitsmaßnahmen und -prozesse durchzuführen.

- 4.6.2 Der Auftragnehmer verpflichtet sich, sich an solchen Penetrationstests auf Verlangen des Auftragnehmers im erforderlichen Umfang zu beteiligen und uneingeschränkt mitzuwirken.

#### **4.7 Überwachung (Art. 30 Abs. 3 lit. e) DORA)**

- 4.7.1 Der Auftraggeber hat das Recht, die Leistungserbringung durch den Auftragnehmer fortlaufend zu überwachen. Hierzu räumt der Auftragnehmer dem Auftraggeber und von ihm beauftragten Dritten ein uneingeschränktes Zugangs-, Inspektions- und Auditrecht ein. Der Auftragnehmer gewährt dem Auftraggeber dabei insbesondere Zugang zu allen Daten und Räumlichkeiten, die mit der Nutzung und Erbringung der Vertragsleistungen zusammenhängen. Dies schließt das Recht auf Anfertigung von Kopien und einschlägiger Unterlagen vor Ort ein, wenn ihnen für die Geschäftstätigkeit des Auftraggebers entscheidende Bedeutung zukommt. Kapitel 4.7.1 gilt entsprechend für Prüfungen durch die Aufsichtsbehörden.
- 4.7.2 Die Parteien vereinbaren, dass die Ausübung der Rechte gemäß Kapitel 4.7.1 („Auditrechte“) nicht durch andere vertragliche Vereinbarungen, insbesondere etwaige Regelungen des Vertrages oder Umsetzungsrichtlinien behindert oder eingeschränkt wird.
- 4.7.3 Soweit Rechte anderer Kunden durch die Ausübung der Auditrechte betroffen werden, können die Parteien ein alternatives Bestätigungsniveau im Einzelfall vereinbaren.
- 4.7.4 Der Auftragnehmer wird bei Vor-Ort-Inspektionen und sonstigen Audits, welche vom Auftraggeber, den Aufsichtsbehörden oder von diesen beauftragten Dritten durchgeführt werden, uneingeschränkt mit diesen zusammenarbeiten.
- 4.7.5 Der Auftraggeber wird dem Auftragnehmer – soweit möglich – den Umfang und das Verfahren entsprechender Prüfungen sowie ihre Häufigkeit mitteilen.

#### **4.8 Exit Management (Art. 30 Abs. 3 lit. f) DORA)**

- 4.8.1 Der Auftragnehmer wird den Auftraggeber bei der Festlegung der Ausstiegsstrategien angemessen unterstützen. Der Auftragnehmer wird insbesondere:
- 4.8.1.1 auf Verlangen des Auftraggebers die Vertragsleistungen über den Beendigungszeitraum hinaus für einen Übergangszeitraum von mindestens 12 Monaten gemäß der im Vertrag vereinbarten Vergütung weiter erbringen, so dass eine ordnungsgemäße Abwicklung, Umstrukturierung oder Überleitung der Vertragsleistungen an einen anderen Dienstleister oder den Auftraggeber selbst (jeweils der „Folgeanbieter“) ohne Unterbrechung der Geschäftstätigkeit und Beeinträchtigung der Kontinuität und Qualität der durch den Auftraggeber gegenüber seinen erbrachten Dienstleistungen erfolgen kann und dabei das Risiko von Störungen in der Organisation des Auftraggebers verringert wird.
- 4.8.1.2 während des Übergangszeitraums die Vertragsleistungen entsprechend der vereinbarten Qualität erbringen und weiterhin alle regulatorischen Anforderungen einhalten;
- 4.8.2 Der Auftragnehmer wird bei der Überleitung der Vertragsleistungen auf den Folgeanbieter im angemessenen Umfang unterstützen.

## **5 Auslagerungsanforderungen (§ 25 b KWG, AT 9 Tz. 7 MaRisk)**

### **5.1 Vertragsgegenstand und Dienstleistungsgüter (AT 9 Tz. 7 lit. a) und lit. e) MaRisk)**

- 5.1.1 Art und Umfang der vom Auftragnehmer insgesamt zu erbringenden Vertragsleistungen ergeben sich aus dem Vertrag.
- 5.1.2 Der Vertrag spezifiziert neben den Vertragsleistungen auch die Dienstleistungsgüter im Hinblick auf die vereinbarten Vertragsleistungen einschließlich möglicher vereinbarter Leistungsziele.

### **5.2 Vertragsbeginn, Dauer, (AT 9 Tz. 7 lit. b) MaRisk)**

- 5.2.1 Der Vertragsbeginn ergibt sich aus den Bestimmungen des Vertrages.
- 5.2.2 Die Dauer des Vertrages ergibt sich aus den Bestimmungen des Vertrages.

### **5.3 Standorte (AT 9 Tz. 7 lit. d) MaRisk)**

Es gelten die Bestimmungen in Kapitel 3.3.

### **5.4 Versicherung (AT 9 Tz. 7 lit. f) MaRisk)**

- 5.4.1 Der Auftragnehmer wird zur Abdeckung etwaiger Schäden eine Haftpflichtversicherung (einschließlich Vermögensschadenshaftpflicht) mit angemessener Deckungssumme abschließen und während der Vertragslaufzeit aufrechterhalten. Auf Verlangen des Auftraggebers wird der Auftragnehmer Existenz und Umfang der Versicherung auf geeignete Art und Weise nachweisen.
- 5.4.2 Konkrete Nachweise von Versicherungsleistungen regelt **Anlage 4**, sofern vom Auftraggeber gefordert.

### **5.5 Notfallmanagementkonzept (AT 9 Tz. 7 lit. g) MaRisk)**

Es gelten die Bestimmungen in Kapitel 4.4.

### **5.6 Koordination, Berichtspflichten und laufende Kontrolle (AT 9 Tz. 7 lit. h MaRisk)**

- 5.6.1 Der Auftragnehmer hat seine Tätigkeit mit der zuständigen Stelle des Auftraggebers zu koordinieren. Die Parteien benennen wechselseitig für die Koordination zuständige entscheidungsbefugte Mitarbeiter und deren Stellvertreter. Die zuständigen entscheidungsbefugten Mitarbeiter sind in **Anlage 3** aufgeführt.
- 5.6.2 Der Auftragnehmer ist verpflichtet, dem Auftraggeber die laufende Steuerung und Überwachung der Vertragsleistung zu ermöglichen und wird auf Wunsch des Auftraggebers über die Erbringung der geschuldeten Leistung(en) schriftlich Bericht erstatten. Der Auftragnehmer wird dem Auftraggeber ab Vertragsbeginn die in **Anlage 4** (Berichtswesen) aufgeführten Berichte mit den dort festgelegten Inhalten zur Verfügung stellen.
- 5.6.3 Im Falle einer Weiterverlagerung auf einen Subunternehmer besteht diese Berichtspflicht auch für Vertragsleistungen des Subunternehmers. Der Auftraggeber kann von dem Auftragnehmer die Erstellung zusätzlicher (d.h. anderer als die in der **Anlage 4** genannten Berichte)

oder die Änderung bestehender Berichte verlangen. Die hierdurch dem Auftragnehmer entstehenden angemessenen, vorhersehbaren und aufwandsbezogenen Kosten werden vom Auftraggeber nach Abstimmung übernommen. Der Auftragnehmer ist verpflichtet, die laufende Kontrolle der Leistungserbringung durch sich selbst sowie, soweit vorhanden, durch Subunternehmer sicherzustellen.

- 5.6.4 Der Auftraggeber ist berechtigt, eine laufende Kontrolle der Leistungserbringung durch den Auftragnehmer durchzuführen. Dabei kann es im Zusammenhang mit den ausgelagerten Aktivitäten und Prozessen insbesondere zusätzliche Auskünfte anfordern.
- 5.6.5 Der Auftragnehmer ist während der Dauer des Vertrages verpflichtet, die für die Erfüllung dieser Zusatzvereinbarung sowie der für den Auftraggeber maßgeblichen Dokumentationspflichten erforderlichen Unterlagen, Daten und sonstigen Informationen im Rahmen der gesetzlichen Aufbewahrungsfristen aufzubewahren sowie auf Verlangen des Auftraggebers auszuhandigen.
- 5.6.6 Der Auftragnehmer ist während der Dauer des Vertrages verpflichtet, (i) gegen sich durch die Aufsichtsbehörde angeordnete aufsichtsrechtliche Maßnahmen und die Ergebnisse aufsichtlicher Prüfungen dem Auftraggeber unverzüglich mitzuteilen und (ii) sich diesbezüglich und hinsichtlich ggf. vorzunehmender Maßnahmen mit dem Auftraggeber abzustimmen. Die Verpflichtung besteht in Bezug auf (i) auch im umgekehrten Fall, sofern die angeordnete(n) aufsichtsrechtliche(n) Maßnahme(n) nach Einschätzung des Auftraggebers für den Auftragnehmer relevant ist/sind.

## **5.7 Interne Revision, Externe Wirtschaftsprüfer, Prüfungsrechte zuständiger Aufsicht-behörden (AT 9 Tz. 7 lit. h), i) MaRisk)**

- 5.7.1 Der Auftraggeber hat ein jederzeitiges, vollumfängliches und ungehindertes Zugangs-, Einseh-, Informations- und Prüfungsrecht hinsichtlich des ausgelagerten Bereichs; dies schließt die Anfertigung von Abschriften und Kopien einschlägiger Unterlagen mit ein. Dem Auftraggeber ist ein Zutritt, Zugang bzw. Zugriff zu allen Räumlichkeiten, Dokumenten, Datenträgern und Systemen beim Auftragnehmer zu gewähren, die die ausgelagerten Aktivitäten und Prozesse betreffen. Die Funktion der Internen Revision wird in Bezug auf die ausgelagerte Vertragsleistung durch die Interne Revision des Auftragnehmers, soweit vorhanden, wahrgenommen. Personen, die beim Auftragnehmer Funktionen der Internen Revision wahrnehmen oder gesetzlich vorgeschriebene oder aufsichtlich angeordnete externe Prüfungen vornehmen, sind gegenüber dem Auftraggeber sowie dessen Prüfern von einer bestehenden Schweigepflicht befreit. Die Interne Revision des Auftragnehmers wird mit der des Auftraggebers vertrauensvoll zusammenarbeiten und die erforderlichen Abstimmungen (u. a. gemeinsam erstellter Prüfungsplan, sofern erforderlich) vornehmen. Der Auftragnehmer stellt sicher, dass die Interne Revision den Anforderungen der MaRisk AT 4.4.3 sowie des BT 2 entspricht. Die Interne Revision des Auftraggebers hat das Recht, sich von der Einhaltung dieser Mindestanforderungen regelmäßig und jederzeit zu überzeugen und darf eigene Ergänzungsprüfungen beim Auftragnehmer durchführen. Im Rahmen ihrer Revisionshandlungen kann die Interne Revision auch auf Nachweise/Zertifikate zurückgreifen, sofern die Aktualität und Eignung der Zertifizierung sowie die zugrundeliegenden Evidenzen zuvor nachgewiesen wurden. Der Auftragnehmer ist verpflichtet, dem Auftraggeber sowie den von diesen beauftragten Abschlussprüfern unaufgefordert die den ausgelagerten Bereich betreffenden Prüfungsberichte,

insbesondere die für den Auftraggeber relevanten Prüfungsergebnisse bzw. Feststellungen, zuzuleiten.

5.7.2 Prüfer zuständiger Bankaufsichtsbehörden (z. B. BaFin oder Deutsche Bundesbank), die beim Auftraggeber aufgrund gesetzlicher Vorgaben tätig werden, Abschlussprüfer des Auftraggebers sowie von diesen mit der Prüfung beauftragte Stellen, haben ein jederzeitiges, vollumfängliches und uneingeschränktes Zugangs-, Einsichts-, Informations- und Prüfungsrecht hinsichtlich der ausgelagerten Aktivitäten und Prozesse; dies schließt die Anfertigung von Abschriften und Kopien einschlägiger Unterlagen mit ein. Diesen Stellen ist ein Zutritt, Zugang bzw. Zugriff zu allen Dokumenten, Datenträgern und Systemen beim Auftragnehmer zu gewähren, die die ausgelagerten Aktivitäten und Prozesse betreffen. Personen, die beim Auftragnehmer Funktionen der Internen Revision wahrnehmen oder gesetzlich vorgeschriebene oder aufsichtlich angeordnete externe Prüfungen vornehmen, sind gegenüber dem Auftraggeber sowie dessen Prüfern von der Schweigepflicht befreit. Der Auftragnehmer hat sich so zu organisieren, dass Rechte Dritter den Pflichten der Sätze 1 bis 2 nicht entgegenstehen.

5.7.3 Alle vorgenannten Rechte bestehen für einen Zeitraum von fünf Jahren nach Beendigung der Auslagerung, beginnend mit dem Ablauf des Geschäftsjahres, in dem der Vertrag beendet wird, fort. Relevante Unterlagen müssen durch den Auftragnehmer beginnend mit dem vorgenannten Zeitpunkt für einen Zeitraum von fünf Jahren und Revisionsberichte und Arbeitsunterlagen von sechs Jahren weiterhin verfügbar bleiben, sofern in dieser Zusatzvereinbarung nichts anderes vereinbart ist. Die sonstigen gesetzlichen Aufbewahrungsfristen bleiben unberührt.

5.7.4 Der Auftraggeber verpflichtet sich seinerseits, dem Auftragnehmer die für die Leistungserbringung des Auftragnehmers relevanten Prüfungsergebnisse seiner Internen Revision, der Aufsichtsbehörden sowie von denen beauftragten Prüfern auf Wunsch zur Verfügung zu stellen.

## **5.8 Weisungen (AT 9 Tz. 7 lit. j) MaRisk)**

5.8.1 Der Auftragnehmer erbringt die vertraglich vereinbarten Vertragsleistungen in eigener Verantwortung.

5.8.2 Der Auftraggeber ist jederzeit unmittelbar und unabhängig von konkurrierenden Weisungsrechten berechtigt, der Geschäftsführung des Auftragnehmers im Zusammenhang mit der Durchführung des Vertrages insbesondere Weisungen im Sinne des § 25a Abs. 2 KWG bzw. zu erteilen und deren Ausführung zu kontrollieren. Die Weisungen bedürfen der Schriftform.

## **5.9 Datenschutz (AT 9 Tz. 7 lit. k) MaRisk)**

Es gelten die Bestimmungen in Kapitel 3.4.

## **5.10 Sicherheits- und Risikomanagement (AT 9 Tz. 7 lit. k) MaRisk)**

5.10.1 Der Auftragnehmer betreibt ein Risikomanagementsystem, um Risiken systematisch zu erkennen und zu steuern. Der im Auftragnehmer etablierte Risikomanagementprozess berücksichtigt die Steuerung, Überwachung und Kontrolle der Risiken, die mit den ausgelagerten Aktivitäten und Prozessen auf den Auftragnehmer übergegangen sind. Sofern vorhanden,

wird der Auftragnehmer diesbezügliche Prüfberichte Dritter dem Auftraggeber unverzüglich zur Verfügung stellen.

- 5.10.2 Der Auftragnehmer hat die banküblichen Sicherheitsanforderungen zu erfüllen. Zu den Sicherheitsanforderungen zählen insbesondere Zugangsbestimmungen zu Räumen und Gebäuden sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen.
- 5.10.3 Der Auftragnehmer stellt durch eine geeignete Aufbau- und Ablauforganisation sicher, dass die Daten des Auftraggebers gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschung, Diebstahl, widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, Zugreifen und andere unbefugte Bearbeitungen geschützt sind. Es stellt ferner entsprechend sicher, dass sicherheitsrelevante Vorfälle umgehend erkannt, bearbeitet und geeignete Gegenmaßnahmen getroffen werden können.
- 5.10.4 Der Auftragnehmer wird den Auftraggeber unverzüglich über jeden sicherheitsrelevanten Vorfall unterrichten. Sicherheitsrelevanter Vorfall ist jeder eingetretene oder drohende Verstoß gegen vertragliche oder gesetzliche Sicherheitsanforderungen sowie alle Vorfälle, Ereignisse oder Umstände, die wesentliche Auswirkungen auf die Sicherheit, Integrität, oder Kontinuität der Vertragsleistungen und/oder die Sicherheit von Daten oder sonstiger Informationen hat oder haben könnte. Zu IKT-Vorfällen siehe Kapitel 3.7.

## **5.11 Kündigung (AT 9 Tz. 7 lit. I) MaRisk)**

- 5.11.1 Die Fristen zur ordentlichen Kündigung des Vertrages ergeben sich aus den Bestimmungen des Vertrages.
- 5.11.2 Jede Partei kann den Vertrag ohne Einhaltung einer Kündigungsfrist aus wichtigem Grund kündigen. Als wichtiger Grund für eine Kündigung gelten insbesondere die folgenden Ereignisse:
  - 5.11.2.1 Der Auftragnehmer erfüllt seine Leistungspflichten trotz Fälligkeit nicht oder nicht ordnungsgemäß. Eine nicht ordnungsgemäße Erfüllung der Leistungspflichten liegt z. B. dann vor, wenn der Auftragnehmer seine Verpflichtungen nicht in Übereinstimmung mit den gesetzlichen, aufsichtsrechtlichen und vertraglichen Anforderungen an eine ordnungsgemäße Leistungserbringung erfüllt, wenn die Sicherheitsstandards verletzt werden oder wenn der Auftragnehmer ein vereinbartes Leistungsniveau wiederholt und nicht nur unerheblich unterschreitet. Die Kündigung ist in diesem Fall in der Regel erst nach erfolglosem Ablauf einer zur Abhilfe bestimmten Frist oder nach erfolgloser Abmahnung zulässig; die Fristsetzung ist jedoch entbehrlich, wenn besondere Umstände vorliegen, die unter Abwägung der beiderseitigen Interessen ein Festhalten des Auftraggebers am Vertrag als unzumutbar erscheinen lassen.
  - 5.11.2.2 Der Auftragnehmer ist zahlungsunfähig, die Insolvenz über das Vermögen des Auftragnehmers wurde beantragt und dieser Antrag ist nicht offensichtlich unbegründet, die

Überschuldung oder Zahlungsunfähigkeit wurde gerichtlich festgestellt, oder die Eröffnung des Insolvenzverfahrens mangels Masse wurde abgelehnt.

- 5.11.2.3 Die zuständige Aufsichtsbehörde verlangt vom Auftraggeber die Kündigung des Vertrages, etwa weil die Aufsichtsbehörde nicht in der Lage ist, infolge des Vertrages, den Auftraggeber effizient zu überwachen.
- 5.11.2.4 Im Falle von erheblichen Mängeln oder Verstößen gegen Datenschutz- oder andere Sicherheitsvorschriften oder -standards, insbesondere Vorschriften bezüglich der Sicherheit von vertraulichen, personenbezogenen oder anderweitig sensiblen Daten oder Informationen.
- 5.11.2.5 Im Falle einer unzulässigen oder durch den Auftraggeber nicht genehmigten Weiterverlagerung von kritischen oder wesentlichen Funktionen gem. Kapitel 5.13.

## **5.12 Exit Management**

- 5.12.1 Im Falle der Beendigung des Vertrages ist der Auftragnehmer verpflichtet, bei der Rückübertragung der ausgelagerten Vertragsleistungen auf den Auftraggeber die erforderlichen Mitwirkungshandlungen zu erbringen, insbesondere Unterlagen, Daten, Dokumente und sonstige Informationen, welche die ausgelagerten Aktivitäten und Prozesse betreffen in geeigneter Form bereit zu stellen und etwaige Restarbeiten vorzunehmen.
- 5.12.2 Auf Verlangen des Auftraggebers ist der Auftragnehmer für einen Zeitraum von bis zu 12 Monaten über den Zeitpunkt der Vertragsbeendigung hinaus verpflichtet, die vertraglichen Hauptleistungen nach Maßgabe des Vertrages zu erbringen. Dadurch soll der Auftraggeber oder ein von ihm benannter Dritter in die Lage versetzt werden, die bisher ausgelagerten Vertragsleistungen entweder selbst oder durch den Dritten erbringen zu lassen. Beide Parteien werden die ihnen zumutbaren Anstrengungen unternehmen, damit die Überleitung zeitnah nach dem Wirksamwerden der Beendigung des Vertrages abgeschlossen werden kann. Hierfür erhält der Auftragnehmer eine aufwandbezogene, angemessene Vergütung. Diese Bestimmungen gelten unabhängig vom Grund der Beendigung, d. h. auch im Falle einer Kündigung aus wichtigem Grund. Weiterhin ist der Auftragnehmer verpflichtet, an einer Konzeption für eine geordnete Übergabe an einen Dritten als Übernehmer hinsichtlich der Durchführung der ausgelagerten Vertragsleistungen aktiv mitzuarbeiten. Der Auftraggeber entscheidet in Abstimmung mit dem Auftragnehmer darüber, ob sich die Übernahme der Vertragsleistungen durch den Übernehmer mit der Leistungserbringung durch den Auftragnehmer zeitlich überschneidet.
- 5.12.3 Die Herausgabepflichten der Kapitel 5.12.2 gelten nicht für die aufgrund gesetzlicher, insbesondere handels-, steuer- und aufsichtsrechtlicher Aufbewahrungsvorschriften für die Eigendokumentation erforderlichen Dokumente. Ein Zurückbehaltungsrecht, gleich aus welchem Rechtsgrund, kann von dem Auftragnehmer nicht geltend gemacht werden.

## **5.13 Weiterverlagerung (AT 9 Tz. 7 lit. m MaRisk)**

Sofern die Weiterverlagerung von Vertragsleistungen kritische oder wesentliche Funktionen betrifft, sollten der Auftragnehmer und der Auftraggeber festlegen, ob der weiter zu verlagernde Teil der Vertragsleistungen an sich kritisch oder wesentlich ist (d. h. einen wesentlichen Teil der kritischen oder wichtigen Funktion darstellt). In diesem Fall ist die Weiterverlagerung nur gestattet, wenn der Auftraggeber der geplanten Weiterverlagerung ausdrücklich zustimmt. Die Zustimmung darf nur aus wichtigem Grund verweigert werden. Ein wichtiger Grund liegt insbesondere vor, wenn die Verlagerung nach der vernünftigen Einschätzung des Auftraggebers

- 5.13.1 die in diesem Zusatzvertrag vereinbarten Prüfungsrechte oder Steuerungs- und Kontrollmöglichkeiten des Auftraggebers oder die Prüfungsrechte und Kontrollmöglichkeiten der Bankenaufsicht oder der Finanzverwaltung einschränkt,
- 5.13.2 die von der Änderung betroffenen Vertragsleistungen und damit verbundenen Risiken des Auftraggebers in einem erheblichen Maße zum Nachteil des Auftraggebers verändert,
- 5.13.3 sich mehr als nur unwesentlich auf die Geschäftsprozesse des Auftraggebers auswirkt,
- 5.13.4 eine Rück- oder Weiterverlagerung der Vertragsleistungen durch den Auftraggeber im Falle der Beendigung des Vertrages erschwert oder ausschließt.
- 5.13.5 Der Auftragnehmer verantwortet und haftet während der Dauer der Subunternehmerschaft für die fortdauernde Zuverlässigkeit und fachliche Eignung des Subunternehmers. Der Subunternehmer gilt als Erfüllungsgehilfe des Auftragnehmers. Bei der Beauftragung von Subunternehmen sind diese ebenfalls auf die Einhaltung der gesetzlichen und sonstigen rechtlichen Verpflichtungen (insb. § 25b KWG i. V. m. MaRisk in jeweils aktueller Fassung) sowie dieser Vertragsbestimmungen zu verpflichten. Dabei ist zu vereinbaren, dass der Auftraggeber, die bei ihm aufgrund gesetzlicher oder behördlicher Vorgaben tätigen Prüfer, die Interne Revision des Auftraggebers und die Bankaufsichtsbehörden, die in dieser Zusatzvereinbarung vereinbarten Informations-, Einsichts-, Prüf-, Kontroll- und Zugangsrechte inhaltsgleich auch beim jeweiligen Subunternehmer des Auftragnehmers wahrnehmen können. Bei Wahrnehmung dieser Rechte durch den Auftraggeber, der bei ihm aufgrund gesetzlicher oder behördlicher Vorgaben tätigen Prüfer, der Internen Revision des Auftraggebers oder der Bankaufsichtsbehörden hat der Auftraggeber dem Auftragnehmer die Prüfung vorab anzuzeigen und über die Ergebnisse der jeweiligen Prüfung unverzüglich zu informieren. Auf Verlangen des Auftraggebers wird der Auftragnehmer die Umsetzung dieser Pflichten bei einer Weiterverlagerung auf geeignete Art und Weise nachweisen. Der Auftragnehmer sichert zu, dass dem Auftraggeber aus der Weiterverlagerung keine höheren Kosten entstehen.
- 5.13.6 Soweit der Auftragnehmer bereits im Zeitpunkt des Vertragsschlusses Subunternehmer mit der Erbringung von nach dem Vertrag geschuldeten Vertragsleistungen ganz oder teilweise beauftragt hat, stimmt der Auftraggeber mit Unterzeichnung dieser Zusatzvereinbarung der Erbringung dieser Vertragsleistungen durch den oder die Subunternehmer im Umfang des Satzes 2 dieses Kapitel 5.13 zu. Eine Übersicht über die beauftragten Subunternehmer und den Umfang der Weiterverlagerung sowie eine Einstufung der Wesentlichkeit ist vom Auftragnehmer mit Abschluss des Zusatzvertrages zu liefern. Der Auftragnehmer sichert zu, dass der oder die Subunternehmer im Rahmen der bestehenden Vertragsverhältnisse ebenfalls zur Einhaltung der in Kapitel 5 bestimmten Anforderungen verpflichtet sind.
- 5.13.7 Der Auftragnehmer darf seinem Subunternehmer (Subunternehmer 1. Stufe) die Weiterverlagerung der Vertragsleistungen auf dessen Subunternehmer (Subunternehmer 2. Stufe) nach Maßgabe des Kapitel 5 gestatten, soweit diese die entsprechende fachliche Eignung und erforderliche Zuverlässigkeit besitzen. Der Auftragnehmer hat insbesondere durch entsprechende vertragliche Regelung dafür Sorge zu tragen, dass auch die Subunternehmer der 2. Stufe verpflichtet sind, die Vertragsleistungen im Einklang mit den gesetzlichen und sonstigen rechtlichen Verpflichtungen sowie den Bestimmungen aus dieser Zusatzvereinbarung zu erbringen. Der Auftragnehmer verantwortet die fachliche Eignung der Subunternehmer der 2. Stufe und haftet dafür. Die Subunternehmer der 2. Stufe gelten als Erfüllungsgehilfen des

Auftragnehmers. Für die Weiterverlagerung der Vertragsleistungen auf Subunternehmer der 3. oder nachfolgender Stufe gelten die Sätze 1 bis 4 entsprechend.

#### **5.14 Informationspflichten (AT 9 Tz. 7 lit. n MaRisk)**

- 5.14.1 Der Auftragnehmer ist verpflichtet, die in Kapitel 5 (**Anlage 3**) genannte zuständige Stelle des Auftraggebers unverzüglich über alle wesentlichen Fehler und Vorkommnisse bei der Erbringung der Vertragsleistungen zu unterrichten.
- 5.14.2 Wesentlich sind insbesondere Fehler und Vorkommnisse, die die ordnungsgemäße Leistungserbringung gefährden können. Dazu gehören insbesondere Fehler und Vorkommnisse, die zu einer erheblichen Schadenshöhe führen können oder die den organisatorischen Arbeitsablauf in erheblicher Weise behindern können, z. B. vorsätzliche Schadenszufügungen von Mitarbeitern, eine massive Häufung von fahrlässig verursachten Störungen, erhebliche Funktionsstörungen in der EDV und personelle Mängel, die erheblichen Einfluss auf die Leistungserbringung haben sowie Verstöße des Auftragnehmers oder der bei diesem beschäftigten Personen gegen die Vorschriften zum Schutz personenbezogener Daten und im Falle eines eingetretenen oder drohenden Datenverlustes. Ebenso ist der Auftragnehmer verpflichtet, die zuständige Stelle rechtzeitig über Entwicklungen zu informieren, die die ordnungsgemäße Erledigung der Vertragsleistungen beeinträchtigen können.

## **6 ANLAGEN**

- a) Anlage 1: Nachhaltigkeitsanforderungen und Unternehmenswerte
- b) Anlage 2: Auftragsverarbeitungsvertrag
- c) Anlage 3: Entscheidungsbefugte Mitarbeiter
- d) Anlage 4: Berichtswesen des Auftragnehmers

Unterschriften:

Auftragnehmer:

<Ort> , den [TT.MM.JJJJ]

Unterschrift:

Auftraggeber:

<Ort> , den [TT.MM.JJJJ]

Unterschrift:

\_\_\_\_\_  
Name des Unterzeichnenden:

<Vorname, Nachname>

\_\_\_\_\_  
Name des Unterzeichnenden:

<Vorname, Nachname>