Vereinbarung zur Auftragsverarbeitung

Als Anlage 5 zum EVB-IT-Cloudvertrag vom [*Datum*]

- nachfolgend „Hauptvertrag" oder „Leistungsbeschreibung" " -

zwischen der
Deutschen Bundesbank,
Frankfurt am Main

- nachfolgend „Verantwortlicher" -

und

[*Vertragspartner*]

- nachfolgend „Auftragsverarbeiter" -

- beide nachfolgend gemeinsam „Vertragsparteien" -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

PRÄAMBEL **3**

§ 1 ANWENDUNGSBEREICH **3**

§ 2 KONKRETISIERUNG DES AUFTRAGSINHALTS **3**

§ 3 DAUER **4**

§4 VERPFLICHTUNGEN UND WEISUNGSBEFUGNIS **4**

§ 5 BEACHTUNG ZWINGENDER GESETZLICHER PFLICHTEN DURCH DEN AUFTRAGSVERARBEITER **6**

§ 6 TECHNISCH-ORGANISATORISCHE MAßNAHMEN UND DEREN KONTROLLE **6**

§ 7 MITTEILUNG BEI VERSTÖßEN DURCH DEN AUFTRAGSVERARBEITER **7**

§ 8 LÖSCHUNG UND RÜCKGABE VON DATEN **8**

§ 9 SUBUNTERNEHMEN **8**

§ 10 DATENSCHUTZKONTROLLE **9**

§ 11 HAFTUNG **9**

§ 12 SCHLUSSBESTIMMUNGEN **9**

ANHANG „WEISUNGSBEFUGNIS“ ZU § 4 UND BENENNUNG DES/ DER ANSPRECHPARTNER/S/IN FÜR DEN DATENSCHUTZ NACH § 5 *(NACH ZUSCHLAGSERTEILUNG AUSZUFÜLLEN)* **11**

ANHANG „TECHNISCH-ORGANISATORISCHE MAßNAHMEN (TOM)“ **12**

ANHANG „SUBUNTERNEHMEN“ ZU § 9 ..... **15**

Präambel

Die Vertragsparteien sind aufgrund des Hauptvertrags ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (*Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG* - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

(1) Die Vereinbarung findet Anwendung auf die Verarbeitung (Art. 4 Nr. 2 DSGVO) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsbeschreibung sind oder im Rahmen von deren Durchführung anfallen und auf Weisung des Verantwortlichen verarbeitet werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

(2) Diese Vereinbarung zur Auftragsdatenverarbeitung gilt bezogen auf ihren Anwendungsbereich vorrangig vor anderen Vereinbarungen und Abreden zwischen Auftraggeber und Auftragnehmer, es sei denn, zwischen den Parteien wird ausdrücklich etwas anderes vereinbart.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten ergeben sich aus

x der Leistungsbeschreibung, der diese Vereinbarung zur Auftragsdatenverarbeitung angefügt ist.

oder

☐ der Leistungsbeschreibung auf Seite(n) XXX des Hauptvertrags .

(2) Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

Name, dienstliche E-Mail-Adresse, Berechtigung

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist (Kategorien betroffener Personen):

Beschäftigte

(4) Im Rahmen der Auftragsverarbeitung werden *keine besonderen* Kategorien von Daten im Sinne von Artikel 9 Abs. 1 DSGVO verarbeitet.

§ 3 Dauer

(1) x Die Dauer dieser Vereinbarung zur Auftragsdatenverarbeitung (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

oder

☐ Die Vereinbarung zur Auftragsdatenverarbeitung beinhaltet eine einmalige Ausführung.

oder

☐ Die Dauer dieser Vereinbarung zur Auftragsdatenverarbeitung(Laufzeit) ist befristet bis zum .....

(2) Der Verantwortliche kann die Vereinbarung zur Auftragsdatenverarbeitung [und den Hauptvertrag] jederzeit ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter seinen Pflichten aus dieser Vereinbarung nicht nachkommt, Bestimmungen der DSGVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will oder ein eingesetzter Subunternehmer den Zutritt des Verantwortlichen oder eines mit der Kontrolle beauftragten Dritten unter Verstoß gegen § 9 verweigert. Die Nichteinhaltung der in dieser Vereinbarung zur Auftragsdatenverarbeitung vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Eine außerordentliche Kündigung aus anderen hierzu berechtigenden wichtigen Gründen bleibt unberührt.

§4 Verpflichtungen und Weisungsbefugnis

(1) Die Vertragsparteien sind verpflichtet, die ihnen durch datenschutzrechtliche Vorschriften (insbesondere die DSGVO) auferlegten Pflichten einzuhalten. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch den Hauptvertrag definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind im Anhang „Weisungsbefugnis" festgelegt.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(7) Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher (oder dokumentierter elektronischer) Zustimmung durch den Verantwortlichen erteilen, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet.

(8) Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(9) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(10) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet
x *der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraumes (EWR)*
oder
☐ *der Bundesrepublik Deutschland*
statt.

(11) Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44ff DSGVO erfüllt sind.

Es wird klargestellt, dass diese Anforderungen zusätzlich zu den Bestimmungen in § 9 gelten, falls ein Subunternehmer beauftragt wird.

Das angemessene Schutzniveau in
_____

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 DSGVO)

oder

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b iVm 47 DSGVO)

oder

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO)

oder

☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e iVm 40 DSGVO)

oder

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f iVm 42 DSGVO)

oder

☐ wird hergestellt durch sonstige Maßnahmen (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DSGVO).

(12) Der Auftragsverarbeiter gewährleistet, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen (oder dokumentierten elektronischen) Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

§ 5 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Sofern der Auftragsverarbeiter der gesetzlichen Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragte/n unterliegt, sind die Kontaktdaten der/des Datenschutzbeauftragten dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme in der Anlage „Weisungsbefugnis zu § 4 und Benennung des/ der Ansprechpartner/s/in für den Datenschutz nach § 5" mitzuteilen. Unterliegt der Auftragsverarbeiter nicht der Benennungspflicht, teilt er dem Verantwortlichen die Kontaktdaten eines Ansprechpartners für den Datenschutz über die Anlage mit.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 6 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen" zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang „Technisch-organisatorische Maßnahmen (TOM)" wird Gegenstand dieser Vereinbarung.

(2) Ergibt eine Prüfung des Verantwortlichen einen Anpassungsbedarf der vom Auftragsverarbeiter zu ergreifenden technisch-organisatorischen Maßnahmen gemäß Artikel 32 DSGVO, sind die Anpassungen vom Auftragsverarbeiter umzusetzen.

(3) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen (TOM)" festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/ Inspektionen, die vom Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen.

(5) Die Überprüfung kann auch auf der Grundlage vorgelegter aktueller Testate, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 DSGVO und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(6) Die Überprüfung kann auch durch eine Inspektion vor Ort erfolgen. Der Verantwortliche kann sich hierzu in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieser Vereinbarung erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(7) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(8) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 7 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung zur Auftragsdatenverarbeitung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs.

2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieser Vereinbarung durchführen.

§ 8 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung des Hauptvertrags, hat der Auftragsverarbeiter sämtliche im Auftrag des Verantwortlichen verarbeitete personenbezogene Daten dem Verantwortlichen zurückzugeben oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu löschen bzw. zu vernichten. Dies umfasst insbesondere dem Auftragsverarbeiter überlassene Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen. Eine weitere Speicherung ist nur zulässig, wenn hierzu eine Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 9 Subunternehmen

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur nach einem der nachfolgenden Verfahren einsetzen:

☐ Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß dieser Vereinbarung zur Auftragsdatenverarbeitung durchführt, ohne vorherige gesonderte schriftliche (oder dokumentierte elektronische) Genehmigung des Verantwortlichen an einen Subunternehmer untervergeben. Der Auftragsverarbeiter reicht den Antrag für die gesonderte Genehmigung mindestens vier Wochen vor der Beauftragung des betreffenden Subunternehmers zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Subunternehmer findet sich im Anhang „Subunternehmen". Die Parteien halten den Anhang jeweils auf dem neuesten Stand.

Der Auftragsverarbeiter erhält die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Subunternehmen, die im Anhang „Subunternehmen" aufgeführt sind. Die Parteien halten den Anhang jeweils auf dem neuesten Stand.

☐ Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Subunternehmen und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des betreffenden Subunternehmens Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem

Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienste. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung zur Auftragsdatenverarbeitung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche (oder dokumentierte elektronische) Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 10 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen zur Erfüllung ihrer bzw. seiner jeweiligen gesetzlich zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag Zugang zu den üblichen Geschäftszeiten zu gewähren. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiterinnen und Mitarbeiter anweisen, mit dem/ der Datenschutzbeauftragten zu kooperieren, insbesondere ihre bzw. seine Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 11 Haftung

Unbeschadet sonstiger vertraglich vereinbarter Haftungsregelungen haften die Parteien bei Verstößen gegen die Bestimmungen in dieser Vereinbarung über die Auftragsdatenverarbeitung bzw. gegen anwendbare datenschutzrechtliche Regelungen nach den insoweit anwendbaren gesetzlichen Vorschriften.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung zur Auftragsdatenverarbeitung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung zur Auftragsdatenverarbeitung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang „Weisungsbefugnis" zu § 4 und Benennung des/ der Ansprechpartner/s/in für den Datenschutz nach § 5 *(nach Zuschlagserteilung auszufüllen)*

zur Vereinbarung zur Auftragsverarbeitung vom *[Datum]*
zwischen XXXXXX XXXX
und *[Vertragspartner]*

Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind nachfolgend festgelegt.

Weisungsberechtigte Personen auf Seiten des Verantwortlichen:

- *X und Y (Weisungsbefugte)*
  (Name, Organisationseinheit, Funktion, Telefon, E-Mail)
- *XX und YY (Stellvertreter)*
  (Name, Organisationseinheit, Funktion, Telefon, E-Mail)

Zum Empfang der Weisungen berechtigte Personen auf Seiten des Auftragsverarbeiters:

- *Z (für … Bereich)*
  (Name, Organisationseinheit, Funktion, Telefon, E-Mail)
- *ZZ (für … Bereich)*
  (Name, Organisationseinheit, Funktion, Telefon, E-Mail)
- *ZZZ(Stellvertreter)*
  (Name, Organisationseinheit, Funktion, Telefon, E-Mail)

Vorgesehene Informationswege, wenn eine Weisung nach Meinung des Auftragsverarbeiters gegen datenschutzrechtliche Vorschriften verstößt:
[Zutreffendes bitte ankreuzen]

- ☐ schriftliche und/oder
- ☐ elektronische und/oder
- ☐ mündliche Information

Weisungen (auch mündliche Weisungen) sind durch die Vertragsparteien zu dokumentieren. Änderungen bei den weisungsbefugten Personen, den zum Weisungsempfang berechtigten Personen und bei den vorgesehenen Informationswegen sind dem Vertragspartner entsprechend unverzüglich anzuzeigen.

Der Auftragsverarbeiter benennt folgende Person als Ansprechpartner für den Datenschutz:

(Name, Funktion (Datenschutzbeauftragte/r oder andere/r Ansprechpartnerin für den Datenschutz) Organisationseinheit, Funktion, Telefon, E-Mail)

Anhang „Technisch-organisatorische Maßnahmen (TOM)"

zur Vereinbarung zur Auftragsverarbeitung vom [*Datum*]
zwischen Deutscher Bundesbank, Frankfurt am Main
und [*Vertragspartner*]

§ 6 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters
Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

[*Hinweis: Alle Maßnahmen sind vertraglich konkret zu bestimmen, pauschale Aussagen und Wiederholung der gesetzlichen Vorschriften genügen nicht.*

Rechtsgrundlage ist Art. 32 DSGVO in dem beschrieben ist, welche technischen und organisatorischen Maßnahmen getroffen werden. So muss der Auftragnehmer unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Es ist ferner sicherzustellen, dass der Auftragnehmer ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung vorweisen muss.
Werden personenbezogene Daten verarbeitet, deren Verarbeitung für die Betroffenen keine besonderen Risiken erwarten lässt, so bietet das IT-Grundschutz-Kompendium des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen (https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html).

Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte als Anlage zum Vertragsbestandteil gemacht werden. In diesem Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen in der Vereinbarung selbst zu wiederholen.

Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, müssen die erforderlichen Maßnahmen in der Vereinbarung detailliert geregelt werden. Aus dem Katalog sollten die einzelnen Maßnahmen in die Vereinbarung übernommen werden. Es handelt sich um keinen abschließenden Maßnahmenkatalog. Insbesondere bei der Verarbeitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich.

Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

- *V e r a n t w o r t l i c h k e i t e n: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.*

- *A b s c h o t t u n g v o n N e t z e n: Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern. Da meist keine absolute Sicherheit zu erreichen ist, müssen derartige Versuche erkannt werden. Technische Komponenten, die in Betracht kommen, sind Firewalls, Intrusion Detection Systeme und insbesondere dem Stand der Technik entsprechende Verschlüsselungsverfahren.*

- *A b h ö r e n d e r K o m m u n i k a t i o n: Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten entsprechend dem Stand der Technik zu verschlüsseln.*

- *A b m e l d e p r o z e d u r e n: Die Abmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.]*

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

a. Vertraulichkeit (Art. 32 Abs 1. lit. b DSGVO)

- Zutrittskontrolle
  Beschreibung des Zutrittskontrollsystems, z. B. Ausweisleser, kontrollierte Schlüsselvergabe, etc.
- Zugangskontrolle
  Maßnahmen, die verhindern, dass die Datenverarbeitungssysteme von Unbefugten genutzt werden können. (Verschlüsselungsverfahren entsprechend dem Stand der Technik.)
- Zugriffskontrolle
  Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungssysteme Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. (Beschreibung von systemimmanenten Sicherungsmechanismen, Verschlüsslungsverfahren entsprechend dem Stand der Technik. Bei Online-Zugriffen des Auftraggebers ist klarzustellen, welche Seite für die Ausgabe und Verwaltung von Zugriffssicherungscodes verantwortlich ist.)
- Trennungskontrolle
  Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
- Pseudonymisierung

b. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. (Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)
- Eingabekontrolle
  Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. (Sämtliche

Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.)

c. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
   - Verfügbarkeitskontrolle
     Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. (Sicherungskopien des Datenbestandes werden in folgenden Verfahren hergestellt: hier Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und Aufbewahrungsort für Back-up-Kopien.)

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.
[z.B. Datenschutz-Management, Incident-Response-Management, datenschutzfreundliche Voreinstellungen, Auftragskontrolle (Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können]

(3) Falls vorhanden, werden folgende Nachweise dieser Vereinbarung angefügt:
[Zutreffendes bitte ankreuzen]

- ☐ Einhaltung von Verhaltensregeln nach Artikel 40 DSGVO
- ☐ Zertifizierung nach Artikel 42 DSGVO
- ☐ Prüfberichte, Testate etc. unabhängiger Prüfer, bspw. Wirtschaftsprüfer, Auditoren, Datenschutzbeauftragte etc.
- ☐ geeignete Zertifizierung durch einen Auditprozess

Anhang „Subunternehmen" zu § 9

Nach § 8 Abs. 1 S. 2 der Vereinbarung sind die zur Erfüllung dieses Vertrages bereits hinzugezogenen Subunternehmen zu bezeichnen. Gem. § 8 Abs. 1 S. 3 der Vereinbarung erklärt sich der Verantwortliche mit deren Beauftragung einverstanden.

Subunternehmen (Name, Anschrift bzw. Sitz)	Datum des Abschlusses der Vereinbarung zur Auftragsverarbeitung	(Teil-)Leistungsgegenstand im Rahmen der Auftragsverarbeitung