

Vertrag über eine Auftragsverarbeitung

zwischen der

Landwirtschaftliche Rentenbank AöR
Theodor-Heuss-Allee 80
60486 Frankfurt am Main

- Verantwortlicher – nachstehend „Auftraggeber“ genannt -

und

Name

Anschrift

- Auftragsverarbeiter – nachstehend „Auftragnehmer“ genannt -

Präambel

Dieser Vertrag über eine Auftragsverarbeitung („Vertrag“) konkretisiert die datenschutzrechtlichen Erfordernisse aufgrund der EU Datenschutz-Grundverordnung („DS-GVO“) sowie des nationalen Bundesdatenschutzgesetzes („BDSG“). Er kommt zur Anwendung, sofern aufgrund der zu erbringenden Leistung auf der Grundlage des Hauptvertrags nicht ausgeschlossen werden kann, dass – wenn auch nur möglicherweise – personenbezogene Daten durch den Auftragnehmer verarbeitet werden (z. B. Erheben, Erfassen Ordnen Speichern, Abfragen, Verwenden). Die für das konkrete Vertragsverhältnis zutreffenden Alternativen sollen angekreuzt und die Leerfelder ggfs. entsprechend des konkreten Auftrags ausgefüllt werden.

§ 1 Gegenstand / Dauer / Kündigungsmöglichkeit

- (1) Der Gegenstand dieses Auftrags ergibt sich aus dem Hauptvertrag (Vertrag über Cloudleistungen – Bankenportal) vom xx.xx.xx, auf welchen hier verwiesen wird.
- (2) Dieser Vertrag tritt mit seiner Unterzeichnung durch beide Parteien in Kraft. Die Dauer des Vertrags richtet sich nach der Dauer des Hauptvertrags. Der Vertrag gilt aber unbeschadet des vorstehenden Satzes so lange weiter, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).
- (3) Die Verpflichtungen aus diesem Vertrag gelten aber auch nach Beendigung des Hauptvertrags weiter, solange der Auftragnehmer nicht sämtliche personenbezogenen Daten des Auftraggebers nach Maßgabe dieses Vertrages herausgegeben, gelöscht oder sonst vernichtet hat.
- (4) Der Auftraggeber kann den Vertrag allerdings jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

§ 2 Konkretisierung des Vertragsinhalts

- (1) **Art** (entsprechend Art. 4 Nr. 2 DS-GVO) und **Zweck** der vorgesehenen Verarbeitung von Daten durch den Auftragnehmer für den Auftraggeber sind
 - ☒ konkret beschrieben in dem Hauptvertrag gem. § 1 Abs. 1.

oder

☐ Nähere Beschreibung des Auftragsgegenstandes:

(2) Die **Art** der verarbeiteten personenbezogenen Daten (entsprechend Art. 4 Nr. 1, 13, 14 und 15 DS-GVO)

☐ ist in dem Hauptvertrag konkret beschrieben unter:

oder

☒ lässt sich in folgende Datenarten/-kategorien aufteilen

☒ Personenstammdaten

☒ Kommunikationsdaten (z.B. Telefon, E-Mail)

☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Kundenhistorie

☒ Vertragsabrechnungs- und Zahlungsdaten

☐ Planungs- und Steuerungsdaten

☐ Auskunftangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)

☒ Logging-Daten

☒ Sonstige: Persönliche Vermerke

(3) Die **Kategorien** der durch die Verarbeitung **betroffenen Personen** entsprechend Art. 4 Nr. 1 DS-GVO

☐ sind in dem Hauptvertrag konkret beschrieben unter:

oder

☒ umfassen:

☒ Kunden

☐ Interessenten

☐ Abonnenten

☒ Beschäftigte

☐ Lieferanten

☐ Handelsvertreter

☒ Ansprechpartner

☐ Antragsteller (natürliche Person)

☐ für den Antragsteller handelnde natürliche Personen

§ 3 Technische und organisatorische Maßnahmen

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen **vor Beginn der Verarbeitung**, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Zum Nachweis der getroffenen Maßnahmen kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheits- oder Datenschutzaudit [z.B. nach BSI-Grundschutz]) vorlegen. Insbesondere die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DS-GVO ist geeignet, um die Erfüllung der vorgenannten Anforderungen nachzuweisen. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) Der Auftragnehmer hat die Sicherheit der personenbezogenen Daten im Sinne der Art. 28 Abs. 3 lit. c), 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Die konkret vom Auftragnehmer getroffenen Maßnahmen sind in **Anhang 1** aufgeführt.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten, Betroffenenrechte

- (1) Der Auftragnehmer darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beaskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken.
- (2) Soweit eine betroffene Person sich bezüglich der in Kapitel III der DS-GVO genannten Rechte oder zwecks Wahrnehmung ihrer weiteren Betroffenenrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (3) Soweit dies jedoch vom Leistungsumfang des Hauptvertrags umfasst ist, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags rechtliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Angaben zum Datenschutzbeauftragten

☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt

☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

b) Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DS-GVO

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte und sonstige Personen ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisungen des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Die Verpflichtung zur Wahrung der Vertraulichkeit besteht **auch nach Beendigung** des Vertrages fort.

c) Zusammenarbeit bei Anfragen der Aufsichtsbehörden

Der Auftragnehmer arbeitet mit dem Auftraggeber auf dessen Anfrage mit der Aufsichtsbehörde bei der Erfüllung von deren Aufgaben zusammen.

d) Information des Auftraggebers über Kontrollhandlungen beim Auftragnehmer

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

e) Unterstützung des Auftraggebers bei Kontrollhandlungen beim Auftraggeber

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person/eines Dritten, einem anderen Anspruch oder einem Informationersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

f) Nachweisbarkeit der technischen und organisatorischen Maßnahmen

Die getroffenen technischen und organisatorischen Maßnahmen müssen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 8 dieses Vertrags nachweisbar sein.

§ 6 Unterauftragsverhältnisse

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag stehen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und rechtskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur unter Einhaltung der Vorgaben aus dieser Vereinbarung beauftragen, d. h. insbesondere, ihm müssen durch den Auftragnehmer das Schutzniveau dieser Vereinbarung nicht unterschreitende Datenschutzpflichten auferlegt werden. Mit Abschluss dieses Vertrages stimmt der Auftraggeber der Einschaltung der in **Anhang 2** aufgeführten Unterauftragnehmer zu, wobei Name und Anschrift sowie der Leistungsbereich des jeweiligen Unterauftragnehmer zu benennen sind. Für nachträgliche Änderungen bzgl. eingesetzter Unterauftragnehmer gelten die Ziffern 15.1 und 15.2 der EVB-IT Cloud AGB entsprechend, sofern die Verarbeitung der in dieser Vereinbarung benannten personenbezogenen Daten von den Veränderungen betroffen ist.
- (3) In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern.

- (4) Die **Weitergabe** von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind **erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung**, insbesondere einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DS-GVO gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vor der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung.
- (5) Eine Auftragsverarbeitung außerhalb der EU bzw. des EWR darf nur erfolgen, wenn die besonderen Voraussetzungen des Kapitel V der DS-GVO erfüllt sind, deren Einhaltung der Auftragnehmer sicherzustellen und dem Auftraggeber auf Anforderung nachzuweisen hat (z. B. Nachweis oder zumindest Bestätigung über Abschluss von SCCs und Transfer Impact Assessments (TIA) / Zertifizierung von US-amerikanischen Dienstleistern nach EU-US Data Privacy Framework etc.).
- (6) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragnehmers.

§ 7 Internationale Datentransfers

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Übermittlung in ein Drittland darf nur erfolgen, wenn der Auftragnehmer die Einhaltung der besonderen Voraussetzungen des Kapitel V der DS-GVO sicherstellt (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Dies hat der Auftragnehmer dem Auftraggeber auf seine Anforderung nachzuweisen (z. B. Nachweis oder zumindest Bestätigung über Abschluss von SCCs und Transfer Impact Assessments (TIA) / Zertifizierung von US-amerikanischen Dienstleistern nach EU-US Data Privacy Framework etc.). Hiervon ausgenommen sind lediglich Datenverarbeitungen, die nicht in den Anwendungsbereich der DS-GVO fallen, weil sie entweder gar keinen Personenbezug aufweisen bzw. es sich um anonymisierte Daten handelt.

§ 8 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht in den zur Erbringung der auftragsgegenständlichen Leistungen genutzten Geschäftsräumen Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb sowie in denen seiner Unterauftragnehmer während der üblichen Betriebs- und Geschäftszeiten zu überzeugen.
- (2) Die Kontrolldichte für die regelmäßige Kontrolle bestimmt der Auftraggeber nach pflichtgemäßem Ermessen unter Berücksichtigung der Interessen des Auftragnehmers und der Bedeutung des Vertrags sowie der unter dem Vertrag durch den Auftragnehmer zu verarbeitenden personenbezogenen Daten.

- (3) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (4) Der Nachweis solcher Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den konkreten Auftrag betreffen, kann erfolgen durch
- ☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
 - ☒ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
 - ☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor);
 - ☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
- (5) Der Auftraggeber strebt priorisiert an, seine Kontrollrechte durch die in Absatz 4 dargestellten Maßnahmen zu erfüllen. Die Berechtigung zur Kontrolle vor Ort aus Absatz 1 bleibt hiervon unberührt.

§ 9 Unterstützungs- und Informationspflichten des Auftragnehmers

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
 - b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich unter Angabe der in Art. 33 Abs. 3 lit. (a) und lit. (d) DS-GVO aufgeführten Einzelinformationen an den Auftraggeber zu melden. Der Auftraggeber wird den Auftragnehmer daher unverzüglich und vollständig informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten mit datenschutzrechtlicher Relevanz feststellt. Darüber hinaus unterrichtet der Auftragnehmer den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder anderen die Daten des Auftraggebers betreffenden Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Der Auftragnehmer wird alle erforderlichen und ihm zumutbaren Maßnahmen zur Sicherung der betroffenen Daten und zur Minderung möglicher Nachteile des Auftraggebers ergreifen,
 - c) die Verpflichtung, den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber

- Aufsichtsbehörden und Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung, soweit der Auftraggeber zur Durchführung verpflichtet ist,
 - e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 10 Weisungsbefugnis des Auftraggebers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen bzw. zur Auftragserfüllung des Hauptvertrags. Weitergehende Verarbeitungen dürfen nur nach Weisungen des Auftraggebers erfolgen, es sei denn der Auftragnehmer ist zu einer anderen Verarbeitung nach dem Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter (Auftragnehmer) unterliegt, hierzu verpflichtet (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter (Auftragnehmer) dem Verantwortlichen (Auftraggeber) 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 S.2 lit. a) DS-GVO).
- (2) Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate von Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Kopien von Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (3) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (4) Weisungsberechtigte Personen des Auftraggebers sind:

Vorname, Name, Organisationseinheit, Telefon
Weisungsempfänger beim Auftragnehmer sind:

Vorname, Name, Organisationseinheit, Telefon

Für die Weisung zu nutzende Kommunikationskanäle:

Genaue postalische Adresse, E-Mail, Telefonnummer

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind der jeweils anderen Partei unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind mindestens für ihre Geltungsdauer aufzubewahren.

- (5) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der

Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

- (6) Erweitert der Auftraggeber seine Weisungen nach Vertragsschluss, sodass eine Verarbeitung personenbezogener Daten durch den Auftragnehmer zu anderen Zwecken als der Erfüllung des Hauptvertrags notwendig wird und entstehen dem Auftragnehmer infolgedessen nachweisbare Mehraufwände, vergütet der Auftraggeber dem Auftragnehmer diese Mehraufwände nach Abstimmung gemäß den vereinbarten Tagessätzen.

§ 11 Löschung und Rückgabe von personenbezogenen Daten

- (1) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftrag stehen, dem Auftraggeber auszuhändigen oder nach dessen vorheriger Zustimmung datenschutzgerecht zu vernichten bzw. die Daten zu löschen, soweit nicht berechtigte Gründe im Sinne von Art. 17 Abs. 3 DS-GVO der Löschung entgegenstehen oder bei Sicherungskopien, die ausschließlich der Datensicherung dienen, bis deren endgültige Löschung erfolgt. Gleiches gilt für Test- und Ausschussmaterial und die an Unterauftragnehmer gelangten Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse. Die **Löschung bzw. Vernichtung** ist **dem Auftraggeber** mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format **zu bestätigen**.
- (2) Der Auftraggeber legt die erforderlichen Maßnahmen zur Löschung gespeicherter Daten nach Beendigung des Auftrages fest. Soweit nach Vertragsbeendigung zusätzliche Kosten durch Herausgabe oder Löschung der Daten des Auftraggebers entstehen, trägt diese der Auftraggeber.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 12 Haftung

Der Auftragnehmer haftet gegenüber dem Auftraggeber für schuldhafte Verletzungen dieser Vereinbarung nach den gesetzlichen Bestimmungen. Es wird auf Art. 82 DS-GVO verwiesen.

§ 13 Sonstiges, Schriftform, Salvatorische Klausel

- (1) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (2) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit

und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DS-GVO liegen.

- (3) Kosten, die dem Auftragnehmer durch die Erfüllung seiner Pflichten aus diesem Vertrag entstehen, trägt der Auftragnehmer selbst und sind im Zweifel mit der Vergütung nach dem Hauptvertrag abgegolten, wenn nicht in diesem Vertrag ausdrücklich etwas Abweichendes geregelt ist.
- (4) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformerfordernis.
- (5) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, verpflichten sich die Parteien, eine Regelung zu finden, die die unwirksame Regelung ersetzt und dieser wirtschaftlich am nächsten kommt.
- (6) Bestandteil dieses Vertrages wird folgender Anhang:
- **Anhang 1** – Technische und organisatorische Maßnahmen
 - **Anhang 2** – Genehmigte Unterauftragnehmer

Ort, Datum, Unterschrift Auftraggeber

Ort, Datum, Unterschrift,
Auftragnehmer

Anhang 1: Technische und organisatorische Maßnahmen i. S. v. Art. 32 DS-GVO

(vom Auftragnehmer bzgl. der tatsächlich getroffenen Maßnahmen zu konkretisieren)

1. Vertraulichkeit (Art. 32 Abs. 1 b) DS-GVO)

- **Zutrittskontrolle**
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- **Trennungskontrolle**
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

2. Pseudonymisierung (Art. 32 Abs. 1 a) DS-GVO, Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

3. Integrität (Art. 32 Abs. 1 b) DS-GVO)

- **Weitergabekontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle**
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 c) DS-GVO)

- **Verfügbarkeitskontrolle**
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/ offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 c) DS-GVO);

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 d) DS-GVO, Art. 25 Abs. 1 DS-GVO)

- **Datenschutz-Management;**

- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**
- **Auftragskontrolle**
Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, Formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Informativ

Anhang 2: Genehmigte Unterauftragnehmer

Firma Unterauftragnehmer	An-schrift/Land	Leistung	Angaben zu geeigneten Garantien bei Daten-übermittlungen in ein Drittland¹

¹ An dieser Stelle kommen insbesondere die Standarddatenschutzklauseln der Kommission gem. Art. 46 Abs. 2 lit. c DS-GVO in Betracht.