Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

Zwischen dem Kunden (als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO; nachfolgend Auftraggeber) und der Creon Solutions GmbH, Aachen (als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO; nachfolgend Auftragnehmer) wird folgender Vertrag über die Verarbeitung personenbezogener Daten im Auftrag geschlossen. Dieser AVV konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Hauptvertrag über IT-Dienstleistungen (nachfolgend Hauptvertrag).

1. Gegenstand, Dauer und Umfang der Verarbeitung

1.1 Gegenstand der Verarbeitung: Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers zum Zwecke der Erfüllung der vereinbarten IT-Dienstleistungen gemäß Hauptvertrag. Dies kann je nach Leistungsumfang insbesondere die Speicherung von Daten auf Serversystemen (Hosting), die Pflege und Wartung von IT-Systemen, die Entwicklung oder der Betrieb von Software-Anwendungen, Support-Dienstleistungen sowie sonstige in Auftrag gegebene Tätigkeiten umfassen.

1.2 Dauer der Verarbeitung: Die Verarbeitung erfolgt für die Dauer des Hauptvertrags. Der AVV tritt mit Unterzeichnung bzw. Abschluss des Hauptvertrags in Kraft und gilt bis zur Beendigung des Hauptvertrags und vollständigen Löschung bzw. Rückgabe der Daten durch den Auftragnehmer. Eine isolierte ordentliche Kündigung dieses AVV ist ausgeschlossen; das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

1.3 Art und Zweck der Verarbeitung: Art und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag. Im Wesentlichen umfasst die Verarbeitung das Erheben, Speichern, Organisieren, Nutzen, Auslesen und Löschen von personenbezogenen Daten, jeweils soweit dies zur vertraglich geschuldeten Leistung (z. B. Betrieb von IT-Systemen oder Implementierung von Software für den Auftraggeber) erforderlich ist. Der Auftragnehmer wird die Daten ausschließlich für die vereinbarten Zwecke verarbeiten. Eine Verarbeitung zu anderen, eigenen Zwecken des Auftragnehmers ist ausgeschlossen.

1.4 Kategorien personenbezogener Daten: Die Kategorien der verarbeiteten personenbezogenen Daten können – abhängig von der konkreten Leistung – insbesondere folgende umfassen:

- Stammdaten: z. B. Namen, Kontaktdaten (Adresse, E-Mail, Telefon) von Kunden, Patienten, Mitarbeitern oder Nutzern des Auftraggebers; Vertrags- und Kundennummern, Login-Kennungen.
- Kommunikationsdaten: z. B. E-Mail-Inhalte, Chat-Protokolle oder Support-Anfragen, soweit sie personenbezogene Informationen enthalten.
- Nutzungs- und Protokolldaten: z. B. Logfiles, IP-Adressen, Nutzungsstatistiken von Software oder Online-Diensten, sofern diese bestimmten Personen zugeordnet sein könnten.
- Sonstige Datenarten: alle weiteren personenbezogenen Daten, die der Auftraggeber dem Auftragnehmer zur Verarbeitung überlässt, wie z. B. Patientenakten oder medizinische Untersuchungsdaten (bei medizinischen Auftraggebern), Bilder oder Dokumente mit Personenbezug, Zahlungsinformationen von Kunden des Auftraggebers, etc. *Besondere Kategorien personenbezogener Daten* (Art. 9 DSGVO) wie Gesundheitsdaten werden vom Auftragnehmer nur verarbeitet, wenn dies Bestandteil des Hauptvertrags ist; der Auftraggeber wird solche sensiblen Daten entsprechend kennzeichnen.

1.5 Kategorien betroffener Personen: Die Kategorien der von der Verarbeitung betroffenen Personen umfassen insbesondere: Kunden, Klienten oder Patienten des Auftraggebers, Mitarbeiter des Auftraggebers, Nutzer von durch den Auftraggeber betriebenen Anwendungen sowie ggf. andere Personen, deren Daten im Auftrag verarbeitet werden (z. B. Lieferantenkontakte, Geschäftspartner). Die konkrete Zuordnung ergibt sich aus dem Hauptvertrag bzw. den Weisungen des Auftraggebers.

1.6 Verarbeitung in der EU / Drittstaatentransfer: Die Verarbeitung personenbezogener Daten durch den Auftragnehmer findet grundsätzlich im Gebiet der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR) statt, insbesondere auf Servern in Deutschland/EU. Eine Verarbeitung in einem Drittland (außerhalb EU/EWR) oder durch einen Dienstleister in einem Drittland erfolgt nur, sofern die Vorgaben der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss oder geeignete Garantien wie EU-Standardvertragsklauseln) und der Auftraggeber zuvor zugestimmt hat. Der Auftraggeber erteilt bereits mit Abschluss dieses AVV die allgemeine Genehmigung, dass der Auftragnehmer Unterauftragnehmer in Drittstaaten einschalten darf, sofern die genannten Bedingungen eingehalten werden (siehe auch Ziffer 5).

2. Pflichten des Auftraggebers (Verantwortlicher)

2.1 Verantwortung für Rechtmäßigkeit: Der Auftraggeber ist für die Rechtmäßigkeit der erhobenen und an den Auftragnehmer übergebenen Daten sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich (Art. 4 Nr. 7 DSGVO). Er hat insbesondere sicherzustellen, dass eine ausreichende Rechtsgrundlage (z. B. Einwilligung oder gesetzliche Erlaubnis) für die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer im Rahmen des Auftrags vorliegt.

2.2 Weisungsrecht: Der Auftraggeber hat das alleinige Recht, in Bezug auf die Verarbeitung der personenbezogenen Daten Weisungen zu erteilen (Art. 28 Abs. 3 lit. a DSGVO). Weisungen und Vorgaben sollen nach Möglichkeit schriftlich oder in Textform (z. B. per E-Mail) erfolgen. Mündliche Weisungen sind vom Auftragnehmer zu dokumentieren oder schriftlich zu bestätigen. Der Auftraggeber wird dem Auftragnehmer bei Vertragsbeginn eine oder mehrere weisungsbefugte Personen benennen.

2.3 Überprüfung der Verarbeitung: Der Auftraggeber hat das Recht und die Pflicht, sich von der Einhaltung der gesetzlichen und vertraglichen Vorgaben durch den Auftragnehmer zu überzeugen. Er kann hierzu in angemessenem Umfang Auskünfte einholen und Kontrollen durchführen (siehe Ziffer 6). Der Auftraggeber wird von diesem Recht in einer Weise Gebrauch machen, die den Betriebsablauf des Auftragnehmers nicht unverhältnismäßig stört.

2.4 Meldung von Fehlern: Der Auftraggeber wird dem Auftragnehmer unverzüglich mitteilen, falls er im Rahmen der Auftragsverarbeitung Fehler oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

2.5 Verzeichnis von Verarbeitungstätigkeiten: Soweit der Auftraggeber gesetzlich dazu verpflichtet ist (Art. 30 Abs. 1 DSGVO), führt er ein Verzeichnis der Verarbeitungstätigkeiten, in das auch die durch den Auftragnehmer im Auftrag durchgeführten Tätigkeiten aufgenommen werden.

3. Pflichten des Auftragnehmers (Auftragsverarbeiter)

Der Auftragnehmer verpflichtet sich, bei der Verarbeitung der personenbezogenen Daten des Auftraggebers die einschlägigen datenschutzrechtlichen Vorgaben, insbesondere der DSGVO und des BDSG, einzuhalten. Im Einzelnen verpflichtet sich der Auftragnehmer zu Folgendem:

- Verarbeitung nur auf Weisung: Der Auftragnehmer wird die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Auftraggebers verarbeiten (Art. 28 Abs. 3 lit. a DSGVO). Dies gilt auch für die Übermittlung an ein Drittland oder an eine internationale

Organisation. Falls der Auftragnehmer gesetzlich (EU-Recht oder Recht eines Mitgliedstaates) zu einer abweichenden Verarbeitung verpflichtet sein sollte, teilt er dem Auftraggeber diese rechtlichen Anforderungen vorab mit (soweit zulässig). Ohne Weisung des Auftraggebers wird der Auftragnehmer keine personenbezogenen Daten des Auftraggebers an Dritte weitergeben.

- Vertraulichkeit: Der Auftragnehmer gewährleistet, dass alle Personen, die bei ihm mit der Verarbeitung der Auftraggeber-Daten betraut sind, vor Beginn der Verarbeitung eine Verpflichtung zur Vertraulichkeit unterzeichnet haben bzw. einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO, i. V. m. § 53 BDSG). Insbesondere werden die Mitarbeiter des Auftragnehmers die Daten des Auftraggebers nicht unbefugt an Dritte weitergeben oder für eigene Zwecke nutzen. Diese Verpflichtung besteht auch nach Beendigung des AVV fort.
- Technische und organisatorische Maßnahmen: Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Maßnahmen (TOM), die gemäß Art. 32 DSGVO erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die personenbezogenen Daten zu gewährleisten. Diese Maßnahmen umfassen insbesondere Zutritts-, Zugriffs- und Zugriffskontrollen, eine angemessene Verschlüsselung oder Pseudonymisierung sensibler Daten, Sicherstellung der Integrität, Verfügbarkeit und Belastbarkeit der Systeme, regelmäßige Datensicherungen, sowie Verfahren zur raschen Wiederherstellung der Verfügbarkeit der Daten nach Zwischenfällen. Die aktuellen technischen und organisatorischen Maßnahmen von Creon sind in einer separaten Anlage oder Dokumentation festgehalten und dem Auftraggeber auf Anfrage zugänglich. Der Auftragnehmer passt die Maßnahmen fortlaufend dem technischen Fortschritt und der Gefährdungslage an, um ein angemessenes Schutzniveau zu gewährleisten.
- Unterstützung bei Betroffenenrechten: Der Auftragnehmer wird den Auftraggeber – soweit möglich – mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflichten zur Wahrung der Rechte der betroffenen Personen nach Kapitel III DSGVO zu erfüllen (Art. 28 Abs. 3 lit. e DSGVO). Insbesondere wird der Auftragnehmer, wenn ihn Auskunfts-, Berichtigungs-, Löschungs- oder Sperrverlangen von Betroffenen unmittelbar erreichen, diese Anfragen nicht selbst beantworten, sondern den Auftraggeber unverzüglich darüber informieren und das weitere Vorgehen abstimmen. Der Auftragnehmer wird dem Auftraggeber alle hierfür erforderlichen Informationen zur Verfügung stellen und soweit nötig bei der Umsetzung von Anweisungen (z. B. Daten löschen oder herausgeben) helfen.
- Meldung von Datenschutzverletzungen: Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden, in Textform zu informieren, sobald ihm Verstöße gegen die ihm obliegenden Datenschutzbestimmungen oder eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO (Datenschutzvorfall) bekannt wird. Diese Meldung hat alle Informationen zu enthalten, die der Auftraggeber seinerseits zur Erfüllung seiner Meldepflicht gegenüber der Aufsichtsbehörde und ggf. Benachrichtigung der Betroffenen nach Art. 33 und 34 DSGVO benötigt. Insbesondere wird der Auftragnehmer mindestens folgende Angaben mitteilen: eine Beschreibung der Art der Verletzung (möglichst mit Kategorien und ungefährer Anzahl der betroffenen Personen und Datensätze), eine Beschreibung der vom Auftragnehmer bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und – falls zutreffend – Maßnahmen zur Abmilderung etwaiger nachteiliger Folgen. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren ferner bei dessen Pflichten zur Unfalluntersuchung, Schadenminderung und Information unterstützen.
- Unterstützung bei Folgenabschätzung und Behördensachen: Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit bei der Einhaltung weiterer in Art. 28 Abs. 3 DSGVO genannter Pflichten. Dazu gehört insbesondere: Unterstützung bei der Erstellung von Datenschutz-Folgenabschätzungen (Art. 35 DSGVO), bei der vorherigen Konsultation mit

Aufsichtsbehörden (Art. 36 DSGVO), sowie bei der Sicherstellung der Datensicherheit (Art. 32 DSGVO) und der Meldepflichten (Art. 33, 34 DSGVO) – jeweils im Rahmen der Leistungserbringung und der vorhandenen Informationen des Auftragnehmers. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Anfrage alle hierfür relevanten Informationen und Nachweise zur Verfügung zu stellen.

- Nachweis und Audits: Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zur Verfügung stellen, um die Einhaltung der Pflichten dieses AVV nachzuweisen, und Kontrollen/Audits nach Ziffer 6 ermöglichen (Art. 28 Abs. 3 lit. h DSGVO). Hierzu kann der Auftragnehmer insbesondere aktuelle Zertifizierungen, Prüfungsberichte oder Audit-Berichte unabhängiger Stellen vorlegen (z. B. ISO 27001, SOC 2 oder TÜV-Prüfberichte), aus denen die Einhaltung angemessener Sicherheitsmaßnahmen hervorgeht. Sollten solche Nachweise dem Auftraggeber nicht ausreichen, kann dieser selbst oder durch einen beauftragten Prüfer Einsicht in die relevanten Unterlagen beim Auftragnehmer nehmen, nach vorheriger Terminabsprache.
- Verzeichnis der Verarbeitungstätigkeiten: Soweit der Auftragnehmer gesetzlich verpflichtet ist (Art. 30 Abs. 2 DSGVO), führt er ein Verzeichnis aller Kategorien von im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die wesentlichen Inhalte dieses Verzeichnisses zur Verfügung, soweit erforderlich.
- Datenschutzbeauftragter: Sofern beim Auftragnehmer gesetzlich erforderlich, hat er einen Datenschutzbeauftragten bestellt. Die Kontaktdaten des Datenschutzbeauftragten von Creon sind in der Datenschutzerklärung von Creon oder auf Anfrage erhältlich. Falls kein Datenschutzbeauftragter bestellt werden muss, benennt der Auftragnehmer dem Auftraggeber einen festen Ansprechpartner für alle Datenschutzfragen im Zusammenhang mit diesem AVV.
- Umgang mit behördlichen Anfragen: Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls eine Prüfung durch die Datenschutz-Aufsichtsbehörde bezüglich der verarbeiteten Daten stattfindet oder wenn eine Behörde bei dem Auftragnehmer Ermittlungen im Zusammenhang mit der Auftragsverarbeitung vornimmt. Er wird keine Informationen herausgeben, ohne den Auftraggeber – soweit rechtlich zulässig – vorab zu benachrichtigen und abzustimmen. Sollte eine Herausgabe von Daten oder Unterlagen des Auftraggebers an Dritte (insbesondere an Behörden) gesetzlich verpflichtend sein (z. B. im Rahmen von Strafverfolgung oder Gefahrenabwehr), wird der Auftragnehmer – soweit erlaubt – den Auftraggeber hierüber informieren.
- Geheimhaltung und Geschäftsgeheimnisse: Der Auftragnehmer ist auch außerhalb datenschutzrechtlicher Vorgaben verpflichtet, Betriebs- und Geschäftsgeheimnisse des Auftraggebers, die ihm im Rahmen der Tätigkeit bekannt werden, vertraulich zu behandeln. Diese Verpflichtung bleibt über das Ende des Vertrags hinaus bestehen.
- Zugang zu Systemen des Auftraggebers: Erhält der Auftragnehmer zur Erfüllung seiner Aufgaben Zugang zu IT-Systemen, Benutzerkonten oder Passwörtern des Auftraggebers, so wird er diese ausschließlich zur Auftragsdurchführung und im Rahmen der Weisungen des Auftraggebers nutzen. Der Auftragnehmer verpflichtet sich, Zugangsdaten sicher zu verwahren und unbefugte Nutzung durch Dritte auszuschließen. Nach Auftragsende oder auf Weisung wird der Zugang deaktiviert oder gelöscht.
- Zugangsdaten und Passwörter: Sofern der Auftragnehmer vom Auftraggeber Zugangsdaten, Passwörter oder andere sicherheitsrelevante Informationen erhält, verpflichtet er sich zur sicheren Aufbewahrung und Nutzung ausschließlich für die Zwecke der Auftragsverarbeitung. Eine Weitergabe an Dritte erfolgt nur mit ausdrücklicher Zustimmung des Auftraggebers. Der Auftragnehmer wird auf Wunsch alle gespeicherten Zugangsdaten nach Beendigung des Auftrags vollständig löschen und dies auf Verlangen dokumentieren.

4. Unterauftragsverhältnisse (Einsatz von Subunternehmern)

4.1 Einschaltung von Unterauftragnehmern: Der Auftragnehmer darf zur Erfüllung seiner vertraglichen Pflichten weitere Auftragsverarbeiter (Subunternehmer) im Sinne von Art. 28 Abs. 2 DSGVO hinzuziehen, soweit dies zur Leistungserbringung erforderlich ist. Hierbei wird der Auftragnehmer den Auftraggeber vorab in Textform informieren, wenn er beabsichtigt, neue Subunternehmer einzusetzen oder bestehende Subunternehmer durch andere zu ersetzen. Der Auftraggeber kann aus berechtigten datenschutzbezogenen Gründen der Einsetzung oder Ablösung eines Subunternehmers innerhalb von 14 Tagen nach Zugang der Information widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Zustimmung des Auftraggebers zur Änderung als erteilt. Im Falle eines berechtigten Widerspruchs wird der Auftragnehmer sich bemühen, eine alternative Lösung zu finden. Ist dies nicht möglich, stehen dem Auftraggeber ggf. besondere Kündigungsrechte zu.

4.2 Aktuell eingesetzte Subunternehmer: Eine Liste der vom Auftragnehmer aktuell im Rahmen dieses AVV eingesetzten Subunternehmer (z. B. Rechenzentrumsbetreiber, Cloud-Dienste) kann dem Auftraggeber auf Wunsch ausgehändigt oder in einer Anlage zu diesem Vertrag beigefügt werden. Der Auftragnehmer sichert zu, dass für alle aufgeführten Subunternehmer eine angemessene vertragliche Vereinbarung nach Art. 28 Abs. 4 DSGVO besteht.

4.3 Vertragliche Weitergabe von Pflichten: Der Auftragnehmer wird mit jedem Subunternehmer einen Auftragsverarbeitungsvertrag abschließen, der den gleichen Datenschutzpflichten unterliegt, wie sie zwischen Auftraggeber und Auftragnehmer vereinbart sind (Art. 28 Abs. 4 DSGVO). Insbesondere wird der Auftragnehmer sicherstellen, dass der Subunternehmer ausreichende Garantien bietet, geeignete technische und organisatorische Maßnahmen umzusetzen, so dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt.

4.4 Sonstige Dienstleister: Leistungen, die der Auftragnehmer von Dritten als Nebenleistungen zur Unterstützung der Auftragsdurchführung in Anspruch nimmt (z. B. Telekommunikationsdienste, Post- und Versanddienstleistungen, Rechenzentrumsinfrastruktur, Reinigungsunternehmen, Wartung und Sicherheit der Gebäude, Entsorgung von Datenträgern, etc.), gelten nicht als Unterauftragsverhältnisse im Sinne von Art. 28 DSGVO. Der Auftragnehmer ist jedoch verpflichtet, auch in diesen Fällen für einen angemessenen Schutz der Daten zu sorgen (z. B. Abschluss von Vertraulichkeitsvereinbarungen oder Auftragsverträgen, soweit erforderlich).

4.5 Haftung der Subunternehmer: Der Auftragnehmer steht dafür ein, dass die eingesetzten Subunternehmer die ihnen übertragenen Pflichten erfüllen. Er haftet gegenüber dem Auftraggeber wie für eigenes Handeln für Handlungen oder Unterlassungen der Subunternehmer.

5. Kontrollrechte des Auftraggebers

5.1 Auditrecht: Der Auftraggeber hat das Recht, Kontrollen durchzuführen oder durch beauftragte Prüfer durchführen zu lassen, um sich von der Einhaltung dieses AVV und der datenschutzrechtlichen Vorschriften beim Auftragnehmer zu überzeugen (Art. 28 Abs. 3 lit. h DSGVO). Dies kann durch Überprüfung vor Ort beim Auftragnehmer (Inspektion) und/oder durch elektronische Anfragebögen/Auskunftsersuchen erfolgen.

5.2 Voranmeldung und Durchführung: Der Auftraggeber soll eine Vorankündigungsfrist von 10 Werktagen für geplante Vor-Ort-Prüfungen einhalten und diese während der üblichen Geschäftszeiten des Auftragnehmers durchführen, damit der Betriebsablauf möglichst wenig gestört wird. Der Auftragnehmer wird die Durchführung der Prüfung im angemessenen Umfang unterstützen. Eine Vor-Ort-Kontrolle darf grundsätzlich höchstens einmal pro Kalenderjahr stattfinden, es sei denn, es liegt ein konkreter Anlass (z. B. Datenschutzvorfall) vor, der eine zusätzliche Kontrolle rechtfertigt.

5.3 Kosten der Kontrolle: Jede Partei trägt ihre eigenen Kosten für eine Durchführung von Audits. Sollte der Aufwand des Auftragnehmers für eine vom Auftraggeber veranlasste Vor-Ort-Prüfung außergewöhnlich hoch sein (z. B. weil ein externer Auditor umfangreiche Tests durchführt, die normale Hilfestellung überschreiten), kann der Auftragnehmer den Mehraufwand nach vorheriger Absprache in Rechnung stellen.

5.4 Nachweise durch den Auftragnehmer: Anstelle von Vor-Ort-Inspektionen kann der Auftraggeber auch vorhandene Zertifizierungen oder Auditberichte des Auftragnehmers als Nachweis heranziehen, sofern diese aktuell sind und einen relevanten Umfang abdecken. Der Auftragnehmer wird dem Auftraggeber auf Wunsch folgende Nachweise zur Verfügung stellen, soweit vorhanden: Zertifikate, Prüfnachweise unabhängiger Stellen (z. B. ISO/IEC 27001, SOC 2), Berichte des Datenschutzbeauftragten, Penetrationstest-Berichte, etc. Falls die vorgelegten Nachweise nicht ausreichen, steht dem Auftraggeber weiterhin das Recht zur eigenen Überprüfung nach Ziffer 5.1 offen.

6. Mitteilungspflichten und Unterstützung bei Verstößen

6.1 Meldung von Verstößen: Wie in Ziffer 3 beschrieben, wird der Auftragnehmer Datenschutzvorfälle oder Verstöße im Zusammenhang mit den vom Auftraggeber überlassenen Daten unverzüglich melden. Der Auftragnehmer hat zudem den Auftraggeber zu informieren, falls zuständige Behörden beim Auftragnehmer Prüfungen durchführen oder Maßnahmen ergreifen, die auch die Auftragsverarbeitung für den Auftraggeber betreffen.

6.2 Unterstützung des Auftraggebers: Im Falle eines Datenschutzvorfalls wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren bei dessen Informationspflichten gegenüber der Aufsichtsbehörde und ggf. betroffenen Personen unterstützen (Art. 33, 34 DSGVO). Er stellt insbesondere die in Ziffer 3 genannten Informationen bereit und wirkt bei der Aufklärung und Schadensbegrenzung mit.

6.3 Anfragen von Betroffenen: Erhält der Auftragnehmer unmittelbar Anfragen von Betroffenen (z. B. Auskunftsersuchen, Löschverlangen) bezüglich der im Auftrag verarbeiteten Daten, wird er diese Anfragen ohne schuldhaftes Zögern an den Auftraggeber weiterleiten. Antworten an die betroffene Person wird – vorbehaltlich anderweitiger Weisung – allein der Auftraggeber erteilen. Der Auftragnehmer wird Betroffene, die sich an ihn wenden, darauf verweisen, dass der Auftraggeber als verantwortliche Stelle zuständig ist.

7. Beendigung des Auftrags und Löschung von Daten

7.1 Vertragsende: Mit Beendigung des Hauptvertrags – gleich aus welchem Grund – endet auch dieser AVV. Der Auftragnehmer wird ab diesem Zeitpunkt keine Verarbeitung der vom Auftraggeber erhaltenen personenbezogenen Daten mehr vornehmen, außer es liegt eine ausdrückliche Weisung des Auftraggebers hierfür vor oder es besteht eine gesetzliche Aufbewahrungspflicht.

7.2 Rückgabe oder Löschung nach Weisung: Nach Beendigung des Vertragsverhältnisses (oder jederzeit auf Verlangen des Auftraggebers) wird der Auftragnehmer alle personenbezogenen Daten, die in seinem Auftrag verarbeitet wurden, nach Wahl des Auftraggebers entweder herausgeben oder löschen (Art. 28 Abs. 3 lit. g DSGVO). Das gleiche gilt für zusammenhängende Datenbestände und Backups. Soweit der Auftraggeber keine konkrete Weisung erteilt, wird der Auftragnehmer standardmäßig eine sichere Löschung aller Auftragsdaten vornehmen.

7.3 Retention aufgrund gesetzlicher Pflichten: Falls der Auftragnehmer aufgrund gesetzlicher Aufbewahrungspflichten (z. B. handels- oder steuerrechtliche Vorgaben) einzelne Daten des Auftraggebers noch nicht löschen darf, tritt an die Stelle der Löschung eine Sperrung der betreffenden Daten. Der Auftragnehmer wird diese Daten nur noch für die gesetzlichen Pflichten

vorhalten und sie für sonstige Zwecke sperren. Nach Ablauf der gesetzlichen Aufbewahrungsfristen wird der Auftragnehmer auch diese Daten unverzüglich löschen.

7.4 Dokumentation der Löschung: Auf Anforderung wird der Auftragnehmer dem Auftraggeber die vollständige Durchführung der Datenlöschung oder Rückgabe schriftlich bestätigen. Der Auftragnehmer darf im Rahmen der gesetzlichen Dokumentationspflichten angemessene Nachweise über die ordnungsgemäße Auftragsverarbeitung (z. B. den Abschlussbericht, Abnahmeprotokolle oder Löschprotokolle) zurückbehalten, wobei solche Unterlagen nur in dem Umfang personenbezogene Daten enthalten dürfen, wie es für den Nachweis erforderlich ist.

7.5 Weitergeltung von Pflichten: Die Pflichten zur Vertraulichkeit und zum Datenschutz bestehen auch nach Beendigung des AVV fort, bis sämtliche personenbezogenen Daten gelöscht wurden. Ziffer 3 (Vertraulichkeit) gilt insoweit über das Vertragsende hinaus.

8. Haftung und Schlussbestimmungen

8.1 Haftungsregeln: Für etwaige Haftungsansprüche zwischen den Parteien im Zusammenhang mit diesem AVV gelten die Haftungsregelungen des Hauptvertrags (insbesondere die in den AGB vereinbarten Haftungsbeschränkungen, siehe dort Ziffer 9) entsprechend. Dies bedeutet insbesondere, dass der Auftragnehmer für Schäden aus der Verletzung dieses AVV nur im Rahmen und in Höhe der im Hauptvertrag vereinbarten Grenzen haftet. Keine Partei haftet für leicht fahrlässige Verstöße gegen lediglich Nebenpflichten aus diesem AVV. Die in diesem AVV enthaltenen Pflichten des Auftragnehmers gelten als wesentliche vertragliche Pflichten im datenschutzrechtlichen Sinne.

8.2 Freistellung bei Verschulden: Macht ein Betroffener oder ein Dritter gegen eine Partei Ansprüche wegen eines Datenschutzverstoßes geltend, der auf einem schuldhaften Verstoß der anderen Partei gegen diesen AVV oder gegen einschlägige Datenschutzbestimmungen beruht, so wird die in Anspruch genommene Partei von der anderen Partei insoweit freigestellt. Diese Freistellung umfasst auch angemessene Kosten der Rechtsverteidigung. Ziffer 11 der AGB (Freistellung durch den Kunden) bleibt unberührt und geht im Zweifel vor, soweit Ansprüche aus dem Verantwortungsbereich des Kunden resultieren.

8.3 Unterordnung unter Hauptvertrag: Dieser AVV ist Bestandteil des Hauptvertrags. Bei etwaigen Widersprüchen zwischen diesem AVV und anderen Vereinbarungen zwischen den Parteien (insbesondere dem Hauptvertrag oder den AGB) gehen die Bestimmungen dieses AVV hinsichtlich der datenschutzrechtlichen Aspekte vor. Im Übrigen ergänzen sich die Regelungen.

8.4 Änderungen und Schriftform: Änderungen, Ergänzungen oder die Aufhebung dieses AVV einschließlich aller Anhänge bedürfen der Schriftform und müssen als solche ausdrücklich gekennzeichnet sein. Dies gilt auch für die Abbedingung dieses Schriftformerfordernisses. Die Parteien arbeiten vertrauensvoll zusammen, um Anpassungen dieses AVV an geänderte gesetzliche Anforderungen vorzunehmen.

8.5 Sonstiges: Sollten einzelne Bestimmungen dieses AVV unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht (Salvatorische Klausel). Die Parteien werden in einem solchen Fall die unwirksame Bestimmung durch eine solche ersetzen, die dem wirtschaftlichen Zweck der unwirksamen möglichst nahekommt. Dieser AVV unterliegt dem in Ziffer 15.1 der AGB genannten Recht (deutsches Recht). Ausschließlicher Gerichtsstand für Streitigkeiten aus diesem AVV ist der in Ziffer 15.1 der AGB genannte Gerichtsstand (soweit zulässig).