All for One Steeb AG,
Gottlieb-Manz-Straße 1, 70794 Filderstadt-Bernhausen,

nachstehend Auftragnehmer genannt.

1 Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Hauptvertrag zwischen den Parteien vom 23.05.2012 in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Diese Anlage findet Anwendung auf sämtliche Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage als Vertragsbestandteil richtet sich nach der Laufzeit des Hauptvertrages.

§ 1 Definition

(1) Personenbezogene Daten

(1a) Im Einzelnen handelt es sich um folgende Arten von Daten, die Aufzahlung ist nicht abschließend:

- Personenstammdaten
- Kommunikationsdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(2) Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

(3) Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden zunächst im Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG).

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von Daten vom Auftragnehmer verlangen.

(3) Die Inhalte dieser Vertragsanlage gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und entsprechend der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(2) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich oder in Textform. Änderungen der getroffenen Vereinbarungen und Verfahrensänderungen sind gemeinsam abzustimmen und festzulegen.

Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Der Auftraggeber hat die weisungsberechtigte Personen dem Auftragnehmer schriftlich zu benennen. Die Dokumentation erfolgt im Betriebsführungshandbuch.

Der zentrale Ansprechpartner für etwaige Weisungen vom Auftraggeber beim Auftragnehmer wird im Betriebsführungshandbuch dokumentiert.

Bei einem Wechsel oder einer längerfristigen Verhinderung des/beider Ansprechpartner ist dem jeweiligen Vertragspartner unverzüglich schriftlich ein Nachfolger bzw. der Vertreter mitzuteilen.

(3) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen

zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen. Dies beinhaltet insbesondere

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),

b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

c) dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

d) dafür Sorge zu tragen, 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 (Weitergabekontrolle),

e) dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

f) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

g) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

Eine Maßnahme nach b) bis d) ist die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen findet sich im Anhang als Anlage zu dieser Vereinbarung.

(4) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4 g) Abs. 2 Satz 1 BDSG notwendigen Angaben zur Verfügung.

(5) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

(6) Beim Auftragnehmer ist als Beauftragter für den Datenschutz Herr Fred Schlindwein/ Ing.büro Frahm GmbH, Osterwiesenstraße 38 in 70794 Filderstadt bestellt.

(7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderer Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.

(8) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind.

(9) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Wiese nachzuweisen.

(10) Der Auftragnehmer erbringt seine Dienstleistungen entweder selbst oder durch die nachfolgend ausdrücklich zugelassenen Subunternehmer aufgrund folgender vertraglicher Vereinbarungen:

- SAP Deutschland AG & Co. KG, Hasso-Plattner-Ring 7, 69190 Walldorf sowie ihre Support-Niederlassungen aufgrund der Pflegevereinbarung über die SAP-Software,
- Global Switch FM GmbH, Eschborner Landstraße 110, 60489 Frankfurt am Main aufgrund eines Mietvertrages,
- E-Shelter Colocation GmbH, Hanauer Landstraße 320, 60314 Frankfurt am Main aufgrund eines Mietvertrages .

(11) Der/die Subunternehmer sind entsprechend der vorliegenden Vereinbarung vertraglich einzubinden.

(12) Die Ver- oder Bearbeitung von Daten vom Auftraggeber in Privatwohnungen einzelner Mitarbeiter vom Auftragnehmer oder derjenigen von Subunternehmern, z. B. durch so genannte Home Offices, ist nur nach vorheriger schriftlicher Zustimmung vom Auftraggeber im Einzelfall gestattet. Soweit Daten in einer Privatwohnung verarbeitet werden, sichert der Auftragnehmer zu, dass die entsprechenden datenschutzrechtlichen Vorschriften eingehalten werden und entsprechende

interne Kontrollen sichergestellt und protokolliert werden.

(13) Die Verarbeitung, Nutzung oder der Zugang zu Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens des europäischen Wirtschaftsraumes statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung vom Auftraggeber und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind. Falls ein Subunternehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen in der vorstehenden Ziffer § 3 Ziffer 9, 10, 11.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber und der Auftragnehmer sind bezüglich der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

(3) Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (Jedermannsverzeichnis) gemäß § 4 g) Abs. 2 Satz 2 BDSG liegt beim Auftraggeber.

(4) Dem Auftraggeber obliegen die aus § 42 a BDSG resultierende Informationspflichten.

(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Einzelweisung fest.

(6) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt dieser der Auftraggeber/Auftragnehmer.

(7) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zusätzlich zu tragen.

§ 5 Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt:

- der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und
- der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten.

§ 6 Kontrollpflichten

Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Hierfür kann er sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich überzeugen und/oder sich ein Testat eines Sachverständigen vorlegen lassen.

§ 7 Salvatorische Klausel

Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder unwirksam werden, insbesondere aufgrund gesetzlicher Änderungen, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien verpflichten sich, anstelle der unwirksamen Bestimmung eine wirksame Bestimmung zu vereinbaren, die Sinn und Zweck der unwirksamen entspricht.

Filderstadt-Bernhausen, 23. Mai 2012

All for One Steeb AG
Geschäftsleitung

Anhang:

Beschreibung der organisatorischen und technischen Maßnahmen (§ 9 Satz BDSG)

Hintergrund des Dokumentes

Die All for One Midmarket AG, als nicht-öffentliche Stelle, die selbst oder im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

In diesem Dokument werden die von der All for One Midmarket AG dazu getroffenen, erforderlichen Maßnahmen beschrieben.

Getroffene Maßnahmen,

die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),

Der Zutritt den Geschäftsräumen der All for One ist nur über ein Zutrittskontrollsystem möglich. Dritte dürfen die Räume nur in Begleitung einer durch All for One autorisierten Person nach vorheriger Anmeldung betreten.

Die Rechenzentren, in denen sich alle zentral genutzten Systeme der All for One befinden, werden als „closed-shop“ betrieben und dürfen nur nach vorheriger Anmeldung und Erteilung einer entsprechenden Berechtigung durch autorisierte Personen betreten werden.

Alle Personen in den Gebäuden sind verpflichtet, sichtbar Zugangskontrollausweise zu tragen. Die eingezäunten Gebäude sind mit Videoüberwachung (mit Archivierung) ausgestattet und verfügen über einen 24/7 Wachdienst. In den Rechenzentrumsgebäuden selbst sind die einzelnen Sicherheitsbereiche mittels elektronischer Zutrittskontrollsysteme (mit Protokollierung) abgesichert.

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

Alle IT-Systeme sind nur via persönlicher Benutzerkennung und Passwort nutzbar. Die Benutzer sind nicht generisch und damit nachvollziehbar Personen zuzuordnen. Passworte müssen auf Grund der Systemeinstellung in regelmäßigen Abständen vom Benutzer geändert werden. Dabei wird systemseitig auf die Eignung (Länge, Zusammensetzung) geachtet und verhindert, dass das gleiche Passwort wiederverwendet werden kann.

Sofern systembedingt generischen Benutzer genutzt werden müssen, wird die Nutzung entsprechend dokumentiert. Dabei wird in einem Protokoll festgehalten:

- Wer hat mit welcher Autorisierung den generischen Benutzer genutzt?
- Wann erfolgte der Zugang und wann war er beendet?
- Warum wurde der generische Benutzer benötigt?
- Welche Tätigkeiten wurden am System durchgeführt?

Das Protokoll wird von der autorisierenden und der durchführenden Person unterzeichnet.

Die Verwaltung der Zugriffsrechte auf Programme, Daten und Dateien erfolgt rollenbasiert durch ein zentrales Berechtigungssystem. Die Einrichtung und der Entzug von Rollen und Berechtigungen erfolgt nur auf Anweisung hierzu besonders autorisierter Personen.

Der Zugang zu Systemen der Auftraggeber ist ausschließlich über eine spezielle Zugangshardware möglich zu dem nur autorisierte Mitarbeiter über ihre zentrale Benutzerberechtigung Zugriff haben.

Im Falle eines Einsatzes aus dem Home-Office oder von anderen Lokationen (z. B. Hotels, Veranstaltungen, Messen) ist sichergestellt, dass der Mitarbeiter nur mittels persönlicher Zugangskennung via VPN auf die IT-Systeme der All for One zugreifen kann.

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

Grundsätzlich erfolgen alle systemseitig notwendigen Tätigkeiten mit nachvollziehbaren Benutzern (siehe Zugangskontrolle). Die Zuordnung der Zugriffsrechte auf Programme, Daten und Dateien erfolgt rollenbasiert. Die Einrichtung und der Entzug dieser Rollen erfolgt nur auf Anweisung hierzu besonders autorisierter Personen.

4. zu 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 (**Weitergabekontrolle**),

Sofern personenbezogene Daten über elektronische Schnittstellen weitergegeben werden, wird die Schnittstelle im Betriebsführungshandbuch gemeinsam mit dem Auftraggeber dokumentiert. Die Weltergabe personenbezogener Daten auf elektronischem Wege erfolgt ausschließlich verschlüsselt.

Bei Systemübernahmen („Transition“) in und aus den Rechenzentren der All for One werden die Datenträger mit den Daten ausschließlich in geeigneten und geschlossenen Behältern mittels ausgewählter Kurierdienste transportiert. Die Übergabe an erfolgt an autorisierte Empfänger. Der Versandvorgang (Absendung und Eingang) wird entsprechend protokolliert.

Der Zugriff auf Systeme der Auftraggeber in den Rechenzentren der All for One erfolgt ausschließlich über ein separat über Firewalls gesichertes, internes Management-Netz, zu dem nur autorisierte Personen über ihre zentrale Benutzerberechtigung (siehe Zugangskontrolle) Zugriff haben.

Der Fernzugriff (Remote Service) auf Systeme des Auftraggebers, die nicht in den Rechenzentren der All for One betrieben werden, erfolgt ausschließlich aus diesem Management-Netz via VPN .

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

Systemzugriffe, die durch den eingeschränkten Benutzerkreis (siehe Zugangskontrolle) von der All for One erfolgen, werden durch Protokollierungen im System nachvollziehbar dokumentiert.

Um weitergehende Protokollierungen zu erhalten, sind entsprechende Funktionen im SAP-System des Auftraggebers zu aktivieren. Die Verantwortung für die Umsetzung dieser Maßnahme verbleibt vollumfänglich beim Auftraggeber

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

Einzelbeauftragungen erfolgen über ein datenbankgestütztes Ticketsystem mittels eines Tickets pro Auftrag. Im Ticket wird die Bearbeitung der Aufträge nachvollziehbar dokumentiert. Tätigkeiten, die aufgrund einer Weisung des Auftraggebers erst nach entsprechender Freigabe oder Vorgaben bearbeitet werden dürfen, werden erst dann bearbeitet, wenn die Freigabe oder Vorgabe vom Auftraggeber im Ticket selbst übermittelt wurde. Die Dokumentation dieser kundenindividuellen Prozesse erfolgt im kundenspezifischen Betriebsführungshandbuch gemeinsam mit dem Auftraggeber.

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

Personenbezogene Daten werden von All for One grundsätzlich auf zenralen Serversystemen gespeichert. Alle zentralen Server- und Managementsysteme der All for One werden ausschließlich in den Rechenzentren der All for One betrieben.

Die Serverräume der All for One in diesen Gebäuden werden mittels Klimatisierung mit einer betriebsoptimalen Raumtemperatur betrieben. Ausreichende Messpunkte in den Serverräumen stellen sicher, dass die automatische Klimatisierung die betriebsoptimale Temperatur hält. Die Stromzuführungen der Rechenzentrumsgebäude und der Serverräume sind unterbrechungsfrei redundant ausgelegt.

USV-Systeme und Dieselaggregate sorgen für den Fall von Unterbrechungen in der Stromversorgung für eine autarke Stromversorgung von mindestens 24 Stunden. Durch geeignete Maßnahmen sind die Gebäude gegen Blitzschlag, Überspannung und Wasserschäden geschützt. Die Brandvermeidung erfolgt gemäß VdS, VDE 0833, DIN 14675.

Ergänzend dazu wird u. a. auch Rauchansaugsystem (RAS) verwendet. Im Fall eines Brandes erfolgt die Löschung durch den Einsatz von Argon.

Der Rechenzentrumsbetrieb für das Gebäude mit dem produktiven Rechenzentrum (1. Rechenzentrumstandort) der All for One ist nach ISO 27001 und DIN ISO 9001 zertifiziert.

Um die IT-Systeme der All for One vor Viren- und Malwarebefall zu schützen, werden auf zentralen und dezentralen IT-Systemen marktübliche Schutzprogramme eingesetzt. Diese Schutzsoftware ist mit Softwarepflegeverträgen hinterlegt und wird automatisiert aktualisiert.

Durch ein standardisiertes Datensicherungskonzept für die Systeme in den Rechenzentren der All for One wird sichergestellt, dass aktuelle Datensicherungen vorhanden sind. Vor Durchführung systemverändernder Maßnahmen wird überprüft, ob die letzte Datensicherung ordnungsgemäß beendet wurde und damit für eine Rücksicherung verfügbar ist.

Bei Systemen, die sich in den Rechenzentren der All for One befinden, werden die Datensicherungen durch die Nutzung des 2. Rechenzentrumsstandortes systemimmanent ausgelagert. Die Entfernung (Luftlinie) vom 1. Rechenzentrumsstandort beträgt zirka 8 km. Die infrastrukturelle Verbindung zwischen den Rechenzentren ist redundant hochverfügbar ausgelegt.

Für die Systeme, die mittels Fernzugriff (Remote Service), betreut werden, verbleibt die Verantwortung für den Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust beim Auftraggeber.

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (**Trennungskontrolle**).

All for One verarbeitet in eigenen IT-Systemen personenbezogene Daten ausschließlich von nachvollziehbaren Benutzern mit ihren in den jeweiligen Systemen zugewiesenen Rollen und Berechtigungen (siehe Zugangskontrolle). In Systemumgebungen, in denen Entwicklungen und Tests stattfinden, werden diese Tätigkeiten auf separaten Entwicklungs- und Testsystemen mit Testdaten durchgeführt.

Die Verantwortung für die Umsetzung weiterer datenschutzrechtlich notwendiger Maßnahmen für die IT-Systeme des Auftraggebers verbleibt vollumfänglich beim Auftraggeber (z. B. SAP Mandanten- und Berechtigungskonzept).