Vereinbarung zur Auftragsverarbeitung

als Anlage zum Vertrag über SRM SW On Demand (nachfolgend „Leistungsvereinbarung“ genannt)

zwischen

– nachfolgend Auftragnehmer genannt –

Firma	Onventis GmbH
Straße / Hausnummer	Gropiusplatz 10
PLZ / Ort	70563 Stuttgart

und – nachfolgend Auftraggeber genannt –

Firma	
Straße / Hausnummer	
PLZ / Ort	

Vertrags Nr.	Vertragsdatum
Version	Ihr Ansprechpartner

Präambel

Die Vertragsparteien gehen mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis entsprechend den Vorgaben der Datenschutzgrundverordnung (EU-Verordnung 2016/679, im Folgenden: „DSGVO“) – gemäß Art. 28 DSGVO ein. Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachstehende Vereinbarung zur Auftragsvereinbarung (im Folgenden „AV-Vereinbarung“).

1 Anwendungsbereich

1.1 Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Auftraggeber der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO ist.

1.2 Im Falle von Regelungswidersprüchen zwischen der Leistungsvereinbarung und der AV-Vereinbarung gehen die Bestimmungen der AV-Vereinbarung vor.

2 Begriffsbestimmung

Diese Vereinbarung bezieht sich nur auf die Durchführung der Verarbeitung von personenbezogenen Daten (nachfolgend auch „Daten" genannt) im Sinne von Art. 4 Nr. 1 (Definition „personenbezogene Daten") und Nr. 2 (Definition „Verarbeitung") DSGVO durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der Erfüllung der Leistungsvereinbarung (Auftragsverarbeitung). Eine weitergehende inhaltliche Aufgabenübertragung wird mit dieser Vereinbarung nicht getroffen.

3 Art, Umfang und Zweck der Auftragsverarbeitung

3.1 Der Gegenstand und die Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten sind in der Leistungsvereinbarung geregelt.

3.2 Folgenden Datenarten oder -kategorien sind Gegenstand der Erhebung, Verarbeitung und/oder Nutzung durch den Auftragnehmer:

- Personenstammdaten, z.B. Name, Adresse, Login Daten, Position
- Kommunikationsdaten, z.B. Telefon, E-Mail
- Unternehmens- und Produktstammdaten, z.B. Mitarbeiter, Adressen, Bankverbindungen, Mitarbeiter, Materialgruppen, Geschäftsbereiche, Steuerdaten, (nur Freelancer) Kompetenzen, Leistungsbeurteilung, Vergütung, Verfügbarkeit
- Lieferantenstammdaten, z.B. Adressen, Ansprechpartner, Bewertungen
- Prozessdaten, z.B. Anfragen, Aufträge, Auktionen, Ausschreibungen, Bedarfe, Bestellungen, Bewertungen, Fristen, Gutschriften, Informationsanfragen, Kataloge, Leistungsnachweise, Lieferabrufe, Lieferpläne, Maßnahmen, Projekte, Rechnungen, Registrierungen, Registrierungsfragen, Reklamationen, Verfügbarkeiten, Verträge, Wareneingänge, Workflows
- Vertragsstammdaten (Vertragsbeziehungen etc.)
- Vertragsbezogene Dokumente, z.B. AGB, Verträge, Bestellungen, Rechnungen, Kunden- bzw. Bestellhistorie
- Logdaten, z.B. Änderungshistorie, Login-Historie
- Kommunikationsdaten, z.B. Chats, Notizen, Technische Einstellungen und Konfigurationen

3.3 Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst Angestellte und freie Mitarbeiter

- des Auftraggebers
- von Lieferanten des Auftraggebers
- von Kunden des Auftraggebers
- von anbietenden bzw. anfragenden Unternehmen

4 Verantwortlichkeit und Weisungen des Auftraggebers

4.1 Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen. Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen schnellstmöglich an den Auftraggeber weiterleiten.

4.2 Der Auftragnehmer darf Daten ausschließlich im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche gesetzeskonforme Anordnung des Auftraggebers. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Auftraggeber danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

4.3 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber schriftlich bestätigt oder geändert wird.

4.4 Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist nicht berechtigt, sie an Dritte weiterzugeben. Kopien werden ohne Wissen des Auftraggebers nicht erstellt.

4.5 Der Auftraggeber führt das Verzeichnis der Verarbeitungstätigkeiten Art. 30 DSGVO. Der Auftragnehmer stellt dem Auftraggeber auf dessen Aufforderung die notwendigen Informationen zur Aufnahme in das Verfahrensverzeichnis zur Verfügung.

4.6 Die Personen des Auftraggebers, welche berechtigt sind, Weisungen gemäß dieser Regelung zu erteilen, sind im Anhang 1: „Ansprechpartner zur Auftragsverarbeitung " festgelegt. Ist eine der darin genannten Personen auf längere Zeit verhindert, scheidet aus dem Unternehmen aus oder steht aus sonstigen Gründen nicht mehr zur Verfügung, ist rechtzeitig eine Ersatzperson zu bestellen und der anderen Vertragspartei unverzüglich zumindest in Textform mitzuteilen.

4.7 Die Meldung von Weisungen gemäß dieser Regelung erfolgt an datenschutz@onventis.de.

5 Pflichten des Auftragnehmers

5.1 Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung wird der Auftragnehmer im Rahmen der Auftragsverarbeitung alle einschlägigen gesetzlichen Pflichten einhalten.

5.2 Der Auftragnehmer ist verpflichtet, das Datengeheimnis zu wahren. Er stellt ferner sicher, dass seine mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter entsprechend zur Vertraulichkeit, insbesondere auf das Datengeheimnis sowie die Einhaltung der Rechte und Pflichten dieser AV-Vereinbarung verpflichtet werden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und in die Schutzbestimmungen der DSGVO und des BDSG. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung. Auf Anforderung des Auftraggebers wird der Auftragnehmer die Erklärungen nach Art. 28 Abs. 3 S. 2 lit. b) DSGVO vorlegen.

5.3 Der Auftragnehmer hat nach Maßgabe des § 38 BDSG bzw. Art. 37 DSGVO einen Datenschutzbeauftragten zu benennen, der seine Tätigkeit gemäß Art. 39 DSGVO ausübt, sofern eine gesetzliche Verpflichtung zur Benennung besteht. Sofern der Auftragnehmer keinen Datenschutzbeauftragten benannt hat, benennt er einen für den Datenschutz zuständigen Mitarbeiter. Die Kontaktdaten eines bestellten Datenschutzbeauftragten bzw. des für den Datenschutz zuständigen Mitarbeiters sind dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

5.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen, Ermittlungen und Maßnahmen durch die Aufsichtsbehörden. Der Auftragnehmer ist verpflichtet, Anfragen von den Datenschutzaufsichtsbehörden unverzüglich an den Datenschutzbeauftragten des Auftraggebers oder an den Auftraggeber weiterzuleiten. Der Auftragnehmer wird den Auftraggeber bei der Erstellung der für diese erforderlichen Dokumentationen im Rahmen seiner Möglichkeiten unterstützen, sofern der Auftraggeber diese Leistungen nicht selbst erbringen kann.

5.5 Der Auftragnehmer ist vorbehaltlich einer gesetzlichen oder behördlichen Verpflichtung ohne entsprechende Weisung des Auftraggebers nicht befugt, Dritten oder dem Betroffenen Auskunft über die verarbeiteten Daten zu geben. Auskunftsersuchen wird der Auftragnehmer unverzüglich an den Auftraggeber weiterleiten. Für die Wahrung der Betroffenenrechte ist der Auftraggeber verantwortlich. Der Auftragnehmer wird jedoch angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte in Kapitel III der DSGVO nachzukommen.

5.6 Der Auftragnehmer wird den Auftraggeber bei der Erstellung der für diese erforderlichen Dokumentationen im Rahmen seiner Möglichkeiten unterstützen, sofern der Auftraggeber diese Leistungen nicht selbst erbringen kann.

6 Technisch-organisatorische Maßnahmen und deren Kontrolle

6.1 Die Vertragsparteien vereinbaren die in Anhang 2 „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang 2 ist Teil dieser Vereinbarung.

6.2 Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang 2 „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6.3 Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise zur Verfügung stellen. Aufgrund der Kontrollverpflichtung des Auftraggebers gemäß Art. 28 und 29 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit der AV-Vereinbarung stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Der Nachweis der Umsetzung solcher Maßnahmenkann auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

6.4 Der Auftraggeber kann sich zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Einhaltung dieser Vereinbarung der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze überzeugen. Die Kontrollen sind dem Auftragnehmer mit einer Vorlaufzeit von nicht weniger als 10 Werktagen (Mo.-Fr. – nicht 24. und 31.12.), bei Vorliegen eines Datensicherheitsvorfalles von nicht weniger als 5 Werktagen anzukündigen. Der Auftraggeber hat hierbei angemessene Rücksicht auf die Betriebsabläufe zu nehmen sowie Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse des Auftragnehmers zu wahren. Der Auftragnehmer wird den Auftraggeber bei der Auftragskontrolle angemessen unterstützen und auf Anforderung hierfür erforderliche Auskünfte bereitstellen. Eine Überprüfung durch Dritte für den Auftraggeber bedarf der vorherigen schriftlichen Zustimmung des Auftragnehmers. Beauftragt der Auftraggeber mit Zustimmung des Auftragnehmers einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich zur Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Geheimhaltungsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

7 Mitteilung bei Verstößen durch den Auftragnehmer

7.1 Bei datenschutzrelevanten Störungen oder Verdacht auf Datenschutzverletzungen bei der Verarbeitung der personenbezogenen Daten ist der Auftragnehmer verpflichtet, den Auftraggeber oder den Datenschutzbeauftragten des Auftraggebers unverzüglich zu informieren. Der Auftraggeber wird auf entsprechenden Hinweis des Auftragnehmers erforderliche Weisungen schriftlich erteilen.

7.2 Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Der Auftragnehmer wird den Auftraggeber bei der Erstellung der für diese erforderlichen Dokumentationen im Rahmen seiner Möglichkeiten unterstützen, sofern der Auftraggeber diese Leistungen nicht selbst erbringen kann.

7.3 Die Personen des Auftraggebers, welche im Falle eines solchen Verstoßes zu informieren sind, sind in Anhang 1: „Ansprechpartner zur Auftragsverarbeitung en" festgelegt. Ist eine der darin genannten Personen auf längere Zeit verhindert, scheidet aus dem Unternehmen aus oder steht aus sonstigen Gründen nicht mehr zur Verfügung, ist rechtzeitig eine Ersatzperson zu bestellen und dem Auftragnehmer über eine E-Mail an datenschutz@onventis.de unverzüglich mitzuteilen.

8 Löschung und Rückgabe von Daten

8.1 Vertragsgegenständlich überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

8.2 Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Auftraggeber auf Anforderung vorzulegen.

8.3 Der Auftragnehmer hat Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

8.4 Der Auftragnehmer bleibt bis zur vollständigen Herausgabe und/oder Löschung vertragsgegenständlicher personenbezogener Daten auch nachvertraglich nach den Regeln dieser Vereinbarung verpflichtet.

9 Unterauftragnehmer (Subunternehmer)

9.1 Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anhang 3 genannten Unterauftragnehmer (Subunternehmer) durchgeführt. Der Auftragnehmer ist darüber hinaus nur nach vorheriger Zustimmung des Auftraggebers in Textform berechtigt, weitere Unterauftragnehmer mit der (vollständigen oder teilweisen) Erbringung der von ihm geschuldeten Leistungen zu beauftragen (Unterauftragsverhältnisse). Der Auftraggeber wird die Zustimmung aus unbilligen Gründen nicht verweigern. Die Zustimmung gilt als erteilt, sofern der Auftraggeber nicht binnen einer Frist von 5 Werktagen auf die Mitteilung des Auftragnehmers über die vorgesehene Beauftragung eines Unterauftragnehmers die begründete Ablehnung der Zustimmung zumindest in Textform erklärt. Der Auftragnehmer ist verpflichtet, Unterauftragnehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Unterauftragnehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

9.2 Der Auftraggeber erteilt die Zustimmung für die in Anhang 3 zu dieser AV-Vereinbarung aufgeführten Unterauftragnehmer. Die Personen des Auftraggebers, welche der Auftragnehmer für die zu erteilende Zustimmung für eine Beauftragung von Unterauftragnehmern mit Nennung von dessen Namen und Anschrift zu informieren hat, sind im Anhang 1: „Ansprechpartner zur Auftragsverarbeitung " festgelegt. Ist eine der darin aufgeführten Personen auf längere Zeit verhindert, scheidet aus dem Unternehmen aus oder steht aus sonstigen Gründen nicht mehr zur Verfügung, ist rechtzeitig eine Ersatzperson zu bestellen und dem Auftragnehmer über eine E-Mail an datenschutz@onventis.de unverzüglich mitzuteilen.

9.3 Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers wie für eigenes Handeln.

9.4 Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Anmietung von Übertragungswegen bei Telekommunikationsanbietern (Carrier), Anmietung von Kollokationsflächen, Wartung und Benutzerservice im Rechenzentrum, Zugriffsmöglichkeit auf Projektmanagementsoftware und Ticketing Software, Supportleistungen durch Dritte z.B. Softwarehersteller und externe Dienstleister betreffend Drittprodukte, Reinigungskräfte, Wachpersonal, Prüfer, Transport von Datenträgern oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen.

9.5 Die Regelungen in dieser Ziffer 9 gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird – ungeachtet des Umstands, dass Datenweitergaben an einen solchen Unterauftragnehmer insbesondere nicht den Privilegierungen des Art. 28 DSGVO unterliegen. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem Unterauftragnehmer, der Auftraggeber-Daten außerhalb des EWR oder der Schweiz verarbeitet oder nutzt, einen Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftrags Verarbeiter in Drittländern vom 5.2.2010 zu schließen.

Sofern der Unterauftragnehmer eine internationale Organisation ist oder seinen Sitz in einem Drittland hat, sind in Bezug auf die Datenübermittlung an den jeweiligen Unterauftragnehmer zum Zweck der Auftragsverarbeitung im Unterauftrag zusätzlich die Vorschriften der Art. 44 ff. DSGVO einzuhalten. Der Auftragnehmer ist sich insbesondere bewusst, dass mangels Angemessenheitsbeschlusses nach Art. 45 Abs. 3 DSGVO oder ordnungsgemäßer Verwendung der EU-Standardvertragsklauseln eine solche Übermittlung grundsätzlich nur zulässig ist, sofern der Unterauftragnehmer geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen, vgl. Art. 46 DSGVO. Der Auftragnehmer ist im Verhältnis zum Auftraggeber für die erforderlichen Garantiemaßnahmen verantwortlich. Der Auftragnehmer ist verpflichtet, die Vorschriften der Art. 44 ff. DSGVO und auch die sonstigen Bestimmungen der DSGVO einzuhalten.

10 Laufzeit der AV-Vereinbarung / Kündigung

10.1 Die Laufzeit und Kündigung dieser AV-Vereinbarung richtet sich nach den Bestimmungen zur Laufzeit und Kündigung der Liefervereinbarung. Eine Kündigung der Liefervereinbarung bewirkt automatisch auch eine Kündigung dieser AV-Vereinbarung. Eine isolierte Kündigung dieser AV-Vereinbarung ist ausgeschlossen. Eine Kündigung aus wichtigem Grund bleibt unberührt.

10.2 Eine Kündigung bedarf zu ihrer Wirksamkeit der Schriftform.

11 Nebenleistungen

Die Ziffern 1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

12 Datenschutzkontrolle

12.1 Der Auftragnehmer verpflichtet sich, dem betrieblichen Datenschutzbeauftragten dem für den Datenschutz zuständigen Mitarbeiters des Auftraggebers zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag Zugang gemäß Ziffer 6.4 dieser AV-Vereinbarung zu gewähren.

12.2 Der Auftragnehmer ist verpflichtet, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 Abs. 3 DSGVO niedergelegten Pflichten auf entsprechende Aufforderung zur Verfügung zu stellen und Überprüfungen zu ermöglichen, die vom Auftraggeber oder einem anderen von diesem zur Verschwiegenheit verpflichteten beauftragten Prüfer nach Maßgabe von Ziffer 6.4 dieser AV-Vereinbarung durchgeführt werden. Die Verpflichtung zur Verschwiegenheit ist dem Auftragnehmer auf entsprechende Aufforderung nachzuweisen.

13 Haftung

13.1 Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers gegen diesen Vertrag sowie gegen die ihn unmittelbar treffenden gesetzlichen Datenschutzverpflichtungen haftet der Auftragnehmer entsprechend den gesetzlichen Haftungsregelungen. Soweit Dritte Ansprüche gegen den Auftraggeber geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftragnehmers gegen diesen Vertrag oder gegen eine ihn unmittelbar treffende gesetzliche Datenschutzverpflichtung haben, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen frei.

13.2 Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diese AV-Vereinbarung oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortliche haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen frei.

13.3 Der Auftragnehmer verpflichtet sich, den Auftraggeber auch von allen etwaigen Geldbußen, die gegen den Auftraggeber verhängt werden, in dem Umfang freizustellen, in dem der Auftragnehmer schuldhaft die alleinige Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

13.4 Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt

14 Gerichtsstand / Anwendbares Recht

14.1 Gerichtsstand für alle Streitigkeiten aus dieser AV-Vereinbarung ist Stuttgart.

14.2 Auf diese Vereinbarung findet das deutsche Recht unter Ausschluss des internationalen Privatrechts Anwendung.

15 Schlussbestimmungen

15.1 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - 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.

15.2 Sollten einzelne Bestimmungen dieser AV-Vereinbarung ganz oder teilweise unwirksam sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Die Vertragsparteien verpflichten sich für diesen Fall, die ungültige Bestimmung durch eine wirksame Bestimmung zu ersetzen, die dem wirtschaftlichen Zweck der ungültigen Bestimmung möglichst nahekommt. Entsprechendes gilt für etwaige Lücken der AV-Vereinbarung.

15.3 Der Anhang 1 „Ansprechpartner des Auftraggebers, der Anhang 2 „Technisch-organisatorische Maßnahmen" und der Anhang 3 „Auflistung Subunternehmer des Auftragnehmers" sind Bestandteil dieser Vereinbarung.

Datum, Ort	Datum, Ort
(Unterschrift des Auftraggebers)	(Unterschrift Onventis GmbH)
Name, Vorname, Funktion	Name, Vorname, Funktion

Ziffer 4.6; Ziffer 7.3 sowie Ziffer 9.2 der Vereinbarung zur Auftragsvereinbarung verweisen zur praktischen Umsetzung der Informationspflichten des Auftragnehmers auf diesen Anhang.

Name	Position	E-Mail-Adresse	Telefonnummer

§1 Gegenstand

Zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DSGVO) sichert der Auftragnehmer dem Auftraggeber das Vorhandensein der nachfolgenden technischen und organisatorischen Maßnahmen zu.

§2 Allgemeine organisatorische Maßnahmen

a. Der Auftragnehmer hat zum Datenschutzbeauftragten bestellt:
Thomas Poole Coats, Onventis GmbH, Gropiusplatz 10, 70563 Stuttgart

b. Beim Auftragnehmer bestehen folgende Regularien zum Datenschutz und zur Vertraulichkeit: Die Mitarbeiter des Auftragnehmers sind zur Einhaltung des Datenschutzes und der Vertraulichkeit verpflichtet. Die benannten Unterlagen können nach Aufforderung beim Auftragnehmer eingesehen werden.

c. Der Auftragnehmer verfügt über folgende Zertifizierungen in den Bereichen Informationstechnik, Datenschutz und Datensicherheit: Die Onventis produktive Umgebung ist gehostet bei ecotel communications ag in einer ISO 27001 zertifiziertes Data-Center. BMEnet GmbH hat:

- die E-Procurement-Plattform der Onventis GmbH, als SRM-Gesamtlösung mit dem Gütesiegel „Supplier Relationship Management“ und
- die Onventis Mobile App Onventis Mobile für mobile Genehmigungs- und Beschaffungsprozesse mit dem Gütesiegel „Mobile Procurement“ ausgezeichnet.

Die Zertifikate können auf Verlangen des Auftraggebers vorgelegt werden.

d. Die Datenverarbeitung durch den Auftragnehmer erfolgt ausschließlich in Deutschland.

§3 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a. Zutrittskontrolle
Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen wie folgt verwehrt:

- Alarmanlage
- Zugangskontrollsystem
- Sicherheitsschlösser
- Schließsystem mit Chipkarte
- Personenkontrolle
- Festlegung befugter Personen
- Fensterversiegelung
- Auf Datenschutz verpflichtetes Reinigungs- und Wartungspersonal
- Beaufsichtigung der Reinigung und Wartung
- Wachpersonal
- Videoüberwachung
- Schlüsselregelung
- Schließsystem mit Transponder
- Manuelles Schließsystem
- Ausweispflicht
- Protokollierung des Zutritts
- Unterteilung in Sicherheitszonen
- Einbruchhemmende Fenster
- Festgelegte Reinigungszeiten
- Geräte- und Gehäuseversiegelung

b. Zugangskontrolle
Die unbefugte Nutzung der Datenverarbeitungssysteme wird durch folgende Maßnahmen verhindert:

- Benutzerkonto für jeden Mitarbeiter
- Authentifikation über Verzeichnisdiente
- Virenschutzlösungen
- Packet Filter Firewall
- Dedizierte Netze für sensible Systeme
- Authentifikation mit Passwort
- Single Sign On
- Zugangsbeschränkung nach Endgerät
- Sperren von BIOS
- Intrusion Detection System
- Application Layer Firewall
- Regelungen bei Ausscheiden von Mitarbeitern

c. Zugriffskontrolle
Nur Berechtigte können die ihnen freigegebenen personenbezogene Daten verarbeiten und nutzen, währenddessen Unbefugte diese Daten weder lesen noch verändern können. Dazu werden folgende Maßnahmen ergriffen:

- dokumentiertes Berechtigungskonzept
- Rollenkonzept
- Differenzierte Berechtigungen für unterschiedliche Transaktionen/Funktionen
- Strenge Passwortrichtlinien
- Protokollierung der Anmeldevorgänge
- Automatische Abmeldevorgänge
- Aufteilung der Administratorrechte unter verschiedenen Personen
- Sichere Aufbewahrung von (Wechsel-) Datenträgern
- systemseitiges Berechtigungskonzept
- Differenzierte Berechtigungen für Datenobjekte
- Regelmäßige Passwortwechsel
- Protokollierung der Datenzugriffe
- Kontensperrung nach mehrmaliger Falscheingabe des Passworts
- Vergabe von Administratorrechten an minimale Anzahl Personen
- Protokollierung von Löschvorgängen

d. Trennungskontrolle
Die Gewährleistung der getrennten Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten wird durch folgende Maßnahmen sichergestellt:

- Physikalisch getrennte Speicherung und Verarbeitung
- Differenzierte Berechtigungen bei der Datenverwaltung
- Logische Kundentrennung
- Attribuierung von Datensätzen nach Zweck der Verarbeitung
- Trennung von Produktiv- und Test-Systemen
- Differenzierung administrativer Aufgaben bei der Datenverwaltung
- Dokumentation der Mandanten und zugehörigen Datenbereiche

e. Pseudonymisierung
Personenbezogene Daten werden in einer Weise verarbeitet, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, es sei denn, ein Personenbezug ist zwingend erforderlich. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

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

a. Weitergabekontrolle
Bei der elektronischen Übertragung oder dem Transport können personenbezogene Daten nicht gelesen, kopiert, verändert oder entfernt werden und der Empfänger der Daten ist jederzeit bekannt, da folgende Maßnahmen ergriffen werden:

- Datenkommunikation über VPN-Tunnel
- Protokollierung der Übermittlungsvorgänge
- Fernlöschung von mobilen Endgeräten
- Transportverschlüsselte Datenübertragung (sichere Übertragung im Internet)
- Dokumentation der Übergabeprozesse bei physischem Transport

b. Eingabekontrolle
Die Kontrolle der Eingabe, Veränderung und Entfernung bzw. Löschung von personenbezogenen Daten wird durch folgende Maßnahmen umgesetzt:

- Arbeiten mit individuellen Benutzerkennungen
- Protokollierung aller Administratoraktivitäten
- Protokollierung der Datenänderungen
- Protokollierung der Zugriffsversuche
- Berechtigungskonzept mit gesonderten Eingabe-, Änderungs- und Löschbefugnissen
- Datenerfassungsanweisungen
- Plausibilitätskontrollen
- Benutzerkennungsbezogene Protokollierung
- Protokollierung der Dateneingaben
- Protokollierung der Datenlöschungen
- Protokollierung gescheiterter Zugriffsversuche
- Sicherung der Protokolldaten gegen Veränderung und Verlust

§ 5 Verfügbarkeit und Belastbarkeit

a. Verfügbarkeitskontrolle
Die verarbeiteten Daten werden durch folgende Maßnahmen gegen zufällige Zerstörung oder Verlust geschützt:

- Sicherungs- und Wiederherstellungskonzept (Backup & Recovery)
- Festgelegte Zuständigkeiten für die Datensicherung
- Notfallplan
- Redundante IT-Systeme
- Unterbrechungsfreie Stromversorgung
- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Automatisches Benachrichtigungssystem
- Schutz vor Wassereinbruch und Hochwasser
- Aufbewahrung der Datensicherung in einem anderen Brandabschnitt
- Regelmäßiger Test der Datenwiederherstellung
- Datenträgerspiegelung (RAID)
- Virtualisierte Infrastruktur
- Überspannungsschutz
- Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen
- Feuerlöscher / automatisches Löschsystem
- Automatisches Notrufsystem
- Nachweis der Eignung der Räumlichkeiten und Bausubstanz

b. Rasche Wiederherstellbarkeit
Alle PSP Instanzen sind Virtuell und können innerhalb Minuten wiederhergestellt außer bei katastrophische Hardware Fehler. In dem Fall wird Wiederherstellung erst möglich bei Neuanschaffung von ESX Hardware.

§ 6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a. Datenschutz-Management

Ein Datenschutzbeauftragter ist weisungsfrei und direkt die Geschäftsleitung unmittelbar unterstellt. Die Aufgabe des Datenschutzbeauftragten ist es m auf die Einhaltung des Bundesdatenschutzgesetzes (BDSG) sowie der europäischen Datenschutzgrundverordnung (DSGVO) sowie andere Vorschriften über den Datenschutz in Onventis hinzuwirken.

Die Aufgaben des DSBs sind insbesondere:

- die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck von der automatisierten Verarbeitung sich rechtzeitig zu informieren, sowie Personen bei der Onventis, die tätig sind bei der Verarbeitung personenbezogene Daten, mit den Vorschriften des BSDGs, der DSGVO sowie andere Vorschriften über den Datenschutz.
- bei aller Datenschutzvorfälle die entsprechende Verantwortlichen zu informieren und bei Datenschutzvorfälle, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, die zuständige Aufsichtsbehörde zu informieren.

b. Auftragskontrolle

Die Sicherstellung der Auftragsdatenverarbeitung nach Weisung des Auftraggebers wird durch folgende Maßnahmen erreicht:

- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Duldung und Unterstützung von Prüfungen durch den Auftraggeber
- Vertragsstrafen vereinbart
- Vernichtung von Daten nach Beendigung des Auftrags
- Rückgabeverfahren für nicht weiter benötigte Unterlagen
- Bestellung einer/eines betrieblichen Datenschutzbeauftragten
- Dokumentation und Auskunft über vorhandene IT-Infrastruktur
- Wirksame Kontrollrechte für den Auftraggeber vereinbart

§ 7 Informationspflicht

Sollte die Anwendung vorstehend genannter Maßnahmen zeitweise länger als 4 Stunden oder vollständig nicht möglich sein, so informiert der Auftragnehmer den Auftraggeber werktags binnen 72 Stunden.

Ziffer 9.2 der Vereinbarung zur Auftragsvereinbarung verweist auf diese Liste der Unterauftragnehmer:

Subunternehmer	Tätigkeit	Zuständiger Onventis Bereich	Standort
Profit GmbH	Dienstleister SAP Schnittstellen	Product & Service	47877 Willich, Deutschland
Chavdar Bambov	Entwickler	Development	Sofia, Bulgarien
Martin Stanchev	Entwickler	Development	Sofia, Bulgarien
SQL Competence	Database Admin	Product & Service	70191 Stuttgart, Deutschland