Anlage Auftragsverarbeitung

zum Softwarepflegevertrag SyncroTESS / SyncroSupply

zwischen der

… GmbH

… [Adresse]

(„Auftraggeber“)

und der

INFORM Institut für Operations Research und Management GmbH,

Pascalstraße 35, 52076 Aachen

(„Auftragnehmer“)

Präambel

Dieser Vertrag zur Auftragsverarbeitung („AVV“) ist Bestandteil des Dienstleistungsvertrages zwischen den Parteien über die Softwarepflege des Systems SyncroTESS / SyncroSupply vom **… [Datum]** einschließlich aller Veränderungen und/oder Verlängerungen **(„Hauptvertrag“)**. Der AVV ist eine Anlage des Hauptvertrags.

1. Gegenstand des AVV

1.1. Geltungsbereich dieses AVV

Soweit der Auftragnehmer im Rahmen der Durchführung des Hauptvertrages Zugang zu den in **Anhang 1** näher definierten personenbezogenen Daten des Auftragsgebers, seiner Mitarbeiter oder Geschäftspartner erhält und/oder für den Auftraggeber in dessen Auftrag verarbeitet, gelten die Bestimmungen dieses AVV.

1.2. Einzelheiten

Einzelheiten zu Umfang, Art und Zweck der vorgesehenen Erhebung und Verwendung personenbezogener Daten sowie zu Art der Daten und Kreis der Betroffenen ergeben sich aus dem Hauptvertrag sowie aus **Anhang 1** dieses AVV.

2. Vertragsdauer

2.1. Dauer

Dieser AVV beginnt mit Inkrafttreten des Hauptvertrags und gilt, bis der Hauptvertrag beendet wurde.

2.2. Kündigung

Der Vertrag kann ohne Einhaltung der Kündigungsfrist gekündigt werden, wenn

- über das Vermögen einer Vertragspartei das Insolvenzverfahren eröffnet, oder die Eröffnung des Insolvenzverfahrens mangels Masse abgelehnt wird,
- eine der Parteien ihre Geschäftstätigkeit einstellt oder

- ein sonstiger wichtiger Grund vorliegt. Ein wichtiger Grund liegt insbesondere dann vor, wenn eine der Vertragsparteien nachhaltig ihre Leistungspflichten oder Nebenpflichten aus diesem Vertragsverhältnis verletzt.

2.3. Sonderkündigungsrecht Auftraggeber

Der Auftraggeber kann den Vertrag 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.

3. Pflichten des Auftragnehmers

3.1. Weisungsgebundenheit

(a) Der Auftragnehmer verarbeitet personenbezogene Daten im Rahmen der im Hauptvertrag geregelten Dienste ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers, in dem in **Anhang 1** vorgesehenen Zweck und Umfang sowie in Übereinstimmung mit den Bestimmungen dieses AVV.

(b) Der Auftraggeber behält sich vor, den Auftrag ergänzende, ändernde oder ersetzende Weisungen in Bezug auf die Verarbeitung zu erteilen. Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt

(c) Soweit Weisungen des Auftraggebers unklar sein sollten, ist der Auftragnehmer verpflichtet, hierüber den Auftraggeber zu informieren und eine Klarstellung einzuholen.

3.2. Zweckänderungen

Für andere als in den Weisungen festgelegte Zwecke dürfen die personenbezogenen Daten nur mit schriftlicher Zustimmung des Auftraggebers verarbeitet werden. Dies gilt insbesondere für eine Weitergabe an Dritte.

3.3. Gesetzeswidrige Weisungen

Ist der Auftragnehmer der Auffassung, dass eine Weisung des Auftraggebers gegen die Datenschutzverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) oder andere datenschutzrechtliche Vorschriften der Europäischen Union oder der Mitgliedstaaten verstößt, weist der Auftragnehmer den Auftraggeber unverzüglich hierauf hin.

3.4. Nicht anwendbar

3.5. Ausnahmen von der Weisungsgebundenheit

Bei gesetzlichen Ausnahmen von der Weisungsgebundenheit des Auftragnehmers gemäß Art. 28 Abs. 3 Satz 2 lit. a) DSGVO informiert der Auftragnehmer den Auftraggeber über auf Grundlage von Rechtsvorschriften erfolgte oder unterbliebene Datenverarbeitungen, es sei denn, die Rechtsvorschrift verbietet dem Auftragnehmer eine Mitteilung.

3.6. Datenschutzrechtliche Bestimmungen

(a) Der Auftragnehmer hält die für ihn geltenden datenschutzrechtlichen Bestimmungen ein.

(b) Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften dieses AVV und der Weisungen des Auftraggebers regelmäßig während der gesamten Vertragslaufzeit.

3.7. Zusammenarbeit mit Aufsichtsbehörden für den Datenschutz

Der Auftragnehmer ermöglicht eine ordnungsgemäße Datenschutzkontrolle und Aufsicht durch die zuständige Aufsichtsbehörde. Insbesondere erteilt er der Aufsichtsbehörde richtig, vollständig und rechtzeitig Auskunft, duldet Prüfungen und (Kontroll-) Maßnahmen und vollzieht Anordnungen der Aufsichtsbehörde. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls sich die Aufsichtsbehörde im Rahmen ihrer Datenschutzkontrolle und Aufsicht unmittelbar an den Auftragnehmer wenden sollte.

3.8. Mitwirkungspflichten

(a) Der Auftragnehmer stellt sicher, dass der Auftraggeber gesetzliche Ansprüche Betroffener aus den Art. 12 bis 22 DSGVO erfüllen kann. Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zu treffen, um den Auftraggeber bei der Beantwortung entsprechender Anträge von Betroffenen zu unterstützen. Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls sich ein Betroffener zum Zwecke der Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung oder seiner Daten unmittelbar an den Auftragnehmer wenden sollte.

(b) Der Auftragnehmer verpflichtet sich, den Auftraggeber bei den zu treffenden Maßnahmen in Bezug auf die Datensicherheit nach Art. 32 DSGVO, bei gegebenenfalls nötigen Meldungen an die Aufsichtsbehörde (Art. 33 DSGVO) oder bei Benachrichtigungen Betroffener (Art. 34 DSGVO), bei der Durchführung von Datenschutz-Folgeabschätzungen (Art. 35 DSGVO) sowie bei der Abstimmung mit Aufsichtsbehörden (Art. 36 DSGVO) zu unterstützen. Insbesondere bei der Erfüllung der Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO) wird der Auftragnehmer dem Auftraggeber die notwendigen Informationen unverzüglich zur Verfügung stellen.

3.9. Informationspflichten

(a) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die dieser benötigt, um die Einhaltung der Vorschriften zur Auftragsverarbeitung gemäß Art. 28 DSGVO dokumentieren und nachweisen zu können.

(b) Der Auftragnehmer informiert den Auftraggeber unverzüglich über datenschutzrelevante Betriebsstörungen, bei Indizien für mögliche oder feststehende Datenschutzverletzungen, bei sonstigen Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten sowie bei Verstößen gegen die Bestimmung dieses AVV durch den Auftragnehmer oder etwaige Subunternehmer des Auftragnehmers. Etwaige Mängel bei der Auftragsverarbeitung sind unverzüglich und unter Erbringung eines schriftlichen Nachweises vom Auftragnehmer zu beseitigen.

(c) Der Auftragnehmer stellt dem Auftraggeber die für das Verzeichnis aller Verarbeitungstätigkeiten nach Art. 30 DSGVO notwendigen Informationen zur Verfügung.

(d) Sollten personenbezogene Daten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich hierrüber zu informieren. Der Auftragnehmer wird die in diesem Zusammenhang Beteiligten unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten bei dem Auftraggeber liegt.

3.10. Vertraulichkeit

(a) Der Auftragnehmer behandelt personenbezogene Daten des Auftraggebers streng vertraulich. Alle zur Datenverarbeitung befugten Personen werden vom Auftragnehmer vor Aufnahme der Tätigkeit mit den Anforderungen des Datenschutzes vertraut gemacht und schriftlich zur Vertraulichkeit und Verschwiegenheit verpflichtet. Diese Verpflichtung sieht auch vor, dass die Vertraulichkeits- beziehungsweise Verschwiegenheitsverpflichtung auch nach Beendigung des Auftrags und auch nach der Beendigung der zwischen diesen Personen und dem Auftraggeber geschlossenen Verträge fortbestehen.

(b) Personenbezogene Daten dürfen vom Auftragnehmer nur solchen Personen zugänglich gemacht werden, die diese personenbezogenen Daten zur Durchführung der Auftragsdatenverwaltung oder des Hauptvertrages kennen oder sonst zu ihnen Zugang haben müssen.

3.11. Datenschutzbeauftragter

Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten benannt. Die Kontaktdaten des Datenschutzbeauftragten finden sich in **Anhang 2**. Änderungen sind dem Auftraggeber unverzüglich schriftlich mitzuteilen.

3.12. Datenexport

Die Datenverarbeitung findet ausschließlich im Bereich der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem Staat statt, dessen Datenschutzniveau die Europäische Kommission per Angemessenheitsbeschluss als dem europäischen angemessen beurteilt hat. Darüber hinaus bedarf jede Verlagerung in ein sonstiges Land („**Drittland**“) der vorherigen schriftlichen Zustimmung des Auftraggebers und darf erfolgen, wenn die besonderen Voraussetzungen für Datenexporte in Drittländer (Art. 44 bis 50 DSGVO) erfüllt sind.

4. Technische und organisatorische Schutzmaßnahmen

4.1. Schutzmaßnahmen

Der Auftragnehmer gewährleistet die Umsetzung der im Rahmen der ordnungsgemäßen Durchführung der Auftragsarbeiten erforderlichen Sicherheitsmaßnahmen. Er trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten, die den Anforderungen der Datenschutzgrundverordnung, insbesondere Art. 32 DSGVO, genügen. Hierzu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- die in **Anhang 3** abgebildeten Maßnahmen treffen. **Anhang 3** ist Bestandteil dieses Vertrages.

4.2. Überprüfungen

Der Auftragnehmer unterhält ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

4.3. Alternative adäquate Maßnahmen

Die erforderlichen 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 und dem Auftraggeber mitzuteilen.

4.4. Angemessenes Schutzniveau

Dem Auftraggeber sind die vom Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen bekannt. Der Auftraggeber trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

4.5. Unterstützung des Auftraggebers bei Dokumentation

Der Auftragnehmer unterstützt den Auftraggeber bei der Dokumentation der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen.

5. Rechte und Pflichten des Auftraggebers

5.1. Einhaltung datenschutzrechtlicher Vorschriften

Der Auftraggeber ist im Rahmen der Umsetzung dieses Auftragsverarbeitungsvertrages für die Einhaltung der Vorgaben der DSGVO sowie anderer einschlägiger Vorschriften zum Datenschutz sowie dafür verantwortlich, dass die gesetzlichen Ansprüche von Betroffenen im Hinblick auf ihre personenbezogenen Daten gewahrt werden.

5.2. Weisungsrecht

Der Auftraggeber hat ein umfassendes Weisungsrecht. Die Weisungsberechtigten beim Auftraggeber und die Weisungsempfangsberechtigten beim Auftragnehmer sind in **Anhang 2** aufgeführt.

6. Kontrollrechte des Auftraggebers und Duldungs- und Mitwirkungspflichten des Auftragnehmers

6.1. Prüfungen

Der Auftraggeber ist berechtigt, vor Beginn der Auftragsverarbeitung und regelmäßig während der Laufzeit dieses AVV vom Auftragnehmer zu verlangen, durch Vorlage von entsprechenden Nachweisen zu belegen, dass die getroffenen technischen und

organisatorischen und in Anhang 3 abgebildeten Maßnahmen sowie die sonstigen, gemäß diesem AVV zu treffenden Maßnahmen zum Datenschutz eingehalten werden.

6.2. Ablauf

Die Prüfung erfolgt nach vorheriger Ankündigung durch den Auftraggeber in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten. Sie hat, soweit möglich, ohne Störung des Betriebsablaufs zu erfolgen.

6.3. Mitwirkungspflichten Auftragnehmer

Der Auftragnehmer wird den Auftraggeber bei der Durchführung von Kontrollen unterstützen und an der vollständigen und zügigen Abwicklung der Kontrolle mitwirken. Der Auftragnehmer ist insbesondere verpflichtet, dem Auftraggeber Zugang zu Datenverarbeitungsanlagen zu gewähren sowie alle Auskünfte zu geben und Unterlagen vorzulegen, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

7. Subunternehmer

7.1. Allgemeine Erlaubnis

Der Auftragnehmer darf weitere Auftragsverarbeiter ohne vorherige gesonderte Genehmigung des Auftraggebers beauftragen.

7.2. Informationspflicht

Der Auftragnehmer informiert den Auftraggeber spätestens 30 Tage vor jeder geplanten Beauftragung weiterer Auftragsverarbeiter. Erfolgt eine Information nicht rechtzeitig, gilt sie als nicht erteilt.

7.3. Inhalt der Information

Der Auftragnehmer informiert den Auftraggeber über Namen und Anschrift des Unterauftragsverarbeiters sowie über Inhalt des geplanten Unterauftrags. Der Auftragnehmer dokumentiert diese Information in geeigneter Weise.

7.4. Widerspruch gegen weitere Auftragnehmer

Der Auftraggeber kann bis zur Beauftragung des Unterauftragsverarbeiters schriftlich Einspruch erheben. In diesem Fall darf der Auftragnehmer den Unterauftragsverarbeiter nicht beauftragen.

7.5. Auswahl und Kontrolle

Subunternehmer sind sorgfältig auszuwählen, insbesondere unter besonderer Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz im Sinne von Art. 32 DSGVO. Sie sind vor der Beauftragung und während der Vertragslaufzeit auf die Einhaltung der gesetzlichen und vertraglichen datenschutzrechtlichen Vorschriften sowie der vereinbarten technischen und organisatorischen Schutzmaßnahmen hin zu kontrollieren. Die Ergebnisse dieser Kontrolle sind zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

7.6. Unterauftragsverarbeitungsvertrag

Vertragliche Vereinbarungen zwischen dem Auftragnehmer und Subunternehmern haben den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieses AVV zu entsprechen. Die Übermittlung von personenbezogenen Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen aus Art. 28 DSGVO erfüllt. Die Beauftragung eines Subunternehmers hat schriftlich zu erfolgen.

7.7. Kontrolle von Subunternehmern

Der Auftragnehmer stellt sicher, dass der Auftraggeber die Prüfungsrechte nach dieser Ziffer 6 auch gegenüber Subunternehmern hat, die der Auftragnehmer einsetzt.

7.8. Einsichtsrecht

Der Auftraggeber ist berechtigt, beim Auftragnehmer Einsicht in dessen Verträge mit Subunternehmern zu nehmen und vom Auftragnehmer die Übersendung einer Kopie dieser Verträge zu verlangen.

7.9. Vorhandene Subunternehmer

Zurzeit sind für den Auftragnehmer die in Anhang 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

8. Rechte an Daten, Datenträgern und Unterlagen

Der Auftraggeber behält im Verhältnis zum Auftragnehmer sämtliche Rechte an den personenbezogenen Daten, Datenträgern und Unterlagen.

9. Berichtigung, Löschung und Herausgabe

9.1. Dauer der Aufbewahrung

Der Auftragnehmer wird die personenbezogenen Daten nur solange aufbewahren, wie vom Auftraggeber angewiesen. Sofern keine konkrete Weisung vorliegt, werden die personenbezogenen Daten vor der Vernichtung nur solange aufbewahrt, wie dies zur Durchführung der jeweiligen Auftragsverarbeitung unter diesem AVV notwendig ist.

9.2. Pflichten des Auftragnehmers bei Aufbewahrung

Der Auftragnehmer hat die ihm zur vertragsgemäßen Vernichtung überlassenen personenbezogenen Daten (insbesondere Datenträger und Unterlagen) unverzüglich zu vernichten und bis zu diesem Zeitpunkt sorgfältig zu verwahren und vor dem unberechtigten Zugriff seiner Mitarbeiter wie auch Dritter zu schützen.

9.3. Vorkehrungen des Auftragnehmers

Der Auftragnehmer trifft die erforderlichen Vorkehrungen, um eine Berichtigung, Löschung und Sperrung der personenbezogenen Daten aufgrund gesetzlicher Anforderungen, auf Verlangen der Aufsichtsbehörde sowie auf Weisung des Auftraggebers vornehmen zu können.

9.4. Rückgabe- und Löschpflicht

Auf Verlangen des Auftraggebers sowie nach Beendigung dieses AVV wird der Auftragnehmer sämtliche personenbezogenen Daten, überlassene Datenträger und Unterlagen, die im Zusammenhang mit dieser Auftragsverarbeitung stehen und personenbezogene Daten des Auftraggebers enthalten, sowie etwaige Kopien davon unverzüglich, spätestens jedoch binnen 14 Tagen nach Aufforderung und Weisung des Auftraggebers bzw. Beendigung der Auftragsverarbeitung, an den Auftraggeber zurückgeben oder unter Einhaltung einschlägiger datenschutzrechtlicher Bestimmungen löschen bzw. vernichten.

9.5. Aufbewahrung von Dokumentationen

Dokumentation, die dem Nachweis der Auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen gesetzlichen oder vertraglich vereinbarten Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

9.6. Test- und Ausschussmaterial

Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer standardmäßig; nur in besonderen, vom Auftraggeber zu bestimmten Fällen erfolgt eine Aufbewahrung bzw. Übergabe. Auf Anforderung weist der Auftragnehmer dem Auftraggeber die datenschutzkonforme Vernichtung des Materials nach.

9.7. Nachweise der Löschung

Der Auftragnehmer weist dem Auftraggeber die Löschung und Zerstörung auf Verlangen schriftlich nach.

10. Haftung

10.1. Außen- und Innenverhältnis

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit dies ihrem Anteil an der Verantwortung entspricht.

10.2. Subunternehmer

Der Auftragnehmer haftet dem Auftraggeber gegenüber entsprechend auch für die Einhaltung der Datenschutzpflichten der Unterauftragnehmer, die er zur Erfüllung seiner Aufgaben einsetzt. Verschulden von Unterauftragnehmern ist dem Auftragnehmer wie eigenes Verschulden zuzurechnen.

10.3. Enthaftung gegenüber Dritten

Der Auftragnehmer ist zum Zwecke der Enthaftung gem. Art. 82 Abs. 3 DSGVO dazu befugt, Details zu Weisungen des Auftraggebers und zur erfolgten Datenverarbeitung offenzulegen. Der Auftraggeber ist dazu verpflichtet, den Auftragnehmer bestmöglich zu unterstützen, damit sich der Auftragnehmer gegenüber dem Dritten nach Art. 82 Abs. 3 DSGVO enthaften kann.

11. Verschwiegenheitspflicht

Die Parteien verpflichten sich, alle gegenseitig mitgeteilten Vorgaben, Daten, Unterlagen, eigene oder gemeinsame Entwicklungsergebnisse, oder sonstige entwicklungs- oder betriebsbezogenen Informationen (auch Preise), bereits im Stadium der Vertragsverhandlungen, während der Vertragsdauer und nachträglich zeitlich unbegrenzt, vertraulich zu behandeln und nicht Dritten zugänglich zu machen. Dies

betrifft insbesondere Tatsachen oder Informationen über Betriebsabläufe, Betriebsergebnisse, Produkte, Geschäftspolitik, Abgaben, Forderungen, organisatorische, soziale oder betriebswirtschaftliche Maßnahmen sowie Daten aus Beschaffungsformen.

12. Anwendbares Recht und Gerichtsstand

12.1. Anwendbares Recht

Dieser AVV unterliegt dem Recht der Bundesrepublik Deutschland.

12.2. Gerichtsstand

Ausschließlicher Gerichtsstand bei allen Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist Aachen. Der Auftraggeber ist berechtigt, den Auftragnehmer auch am Gericht des Sitzes des Auftragnehmers zu verklagen.

13. Sonstige Bestimmungen

13.1. Vorgaben der Kommission oder Aufsichtsbehörde

Sollten die EU-Kommission oder die zuständige Aufsichtsbehörde Standardklauseln für Auftragsverarbeitungsverträge festlegen, werden sich die Parteien im erforderlichen Umfang auf eine mögliche Anpassung dieser Vereinbarung an die Standardklauseln verständigen.

13.2. Kosten

Alle Leistungen des Auftragnehmers in Zusammenhang mit der Erfüllung seiner Pflichten unter diesem AVV sind mit der Vergütung aus dem Hauptvertrag abgegolten.

13.3. Kollisionsregel

Im Falle eines Widerspruchs zwischen dem Hauptvertrag und diesem AVV geht dieser AVV vor, soweit die Regelung des AVV die Verarbeitung personenbezogener Daten betrifft. Sollten einzelne Teile dieses AVV unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelung des AVV oder des Hauptvertrages nicht.

13.4. Ausschluss Zurückbehaltungsrecht

Die Einrede des Zurückhaltungsrechts i. S. v. § 273 BGB ist hinsichtlich der verarbeiteten personenbezogenen Daten und der dazugehörigen Unterlagen und Datenträger ausgeschlossen.

13.5. Gesetzliche Verpflichtungen oder Anordnungen

Verpflichtungen des Auftragnehmers aufgrund gesetzlicher Vorschriften oder behördlicher oder gerichtlicher Anordnungen bleiben von diesem AVV unberührt.

_____	_____
Datum	*Datum*
_____	_____
Unterschrift Auftraggeber	*Unterschrift Auftragnehmer*
_____	_____
Name in Druckbuchstaben	*Name in Druckbuchstaben*

Anhang 1

Angaben zur Datenverarbeitung

1. Gegenstand und Dauer der Verarbeitung

[Hier beschreiben die Parteien den Hintergrund der Verarbeitung (z. B. die Erhebung von Kundendaten) und die ungefähre Dauer der Verarbeitung.]

2. Art und Zweck der Verarbeitung

[Die Parteien legen an dieser Stelle fest, welche Art der Datenverarbeitung geplant ist (Erheben, Erfassen, Organisation, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermitteln, Verbreiten oder eine andere Form des Bereitstellens, Abgleichen oder Verknüpfen, Einschränken, Löschen oder Vernichten; vgl. Art. 4 Nr. 2 DSGVO) und zu welchem Zweck dies geplant ist (die Beschreibung des Zwecks erfolgt an dieser Stelle detaillierter als bei Nr. 1).]

3. Art der personenbezogenen Daten

[Die Parteien führen hier auf, welche Kategorien personenbezogener Daten betroffen sind. Besonders heben sie hervor, ob besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) oder Daten über Straftaten oder Verurteilungen (Art. 10 DSGVO) betroffen sind.]

4. Kategorien von Betroffenen

[Die Parteien legen fest, welche Kategorien von natürlichen Personen von der Datenverarbeitung betroffen sind (z. B. Mitarbeiter und ehemalige Mitarbeiter des Unternehmens, Kunden des Unternehmens).]

Anhang 2

Datenschutzbeauftragter, Weisungsberechtigte, Weisungsempfänger, Subunternehmer

1. Datenschutzbeauftragter

Der Auftragnehmer hat derzeit folgenden Datenschutzbeauftragten bestellt

Dr. Oliver Meyer-van Raay
V-Formation GmbH, Stephanienstrasse 18, 76133 Karlsruhe
Telefon: +49 721 17029034
E-Mail: om@v-formation.gmbh

2. Weisungsberechtigte

Weisungsberechtigt sind auf Seiten des Auftraggebers der verantwortliche Projektleiter und dessen Vorgesetze.

3. Weisungsempfänger

Berechtigt Weisungen des Auftraggebers zu empfangen ist der Supportmanager.

4. Subunternehmer

Zum Zeitpunkt des Vertragsschlusses sind keine Unterauftragnehmer benannt.

NAME	ANSCHRIFT	AUFTRAGSINHALT
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy L-1855 Luxemburg	Betrieb des Rechenzentrums

Anhang 3

Technisch-organisatorische (Sicherheits-) Maßnahmen bei der INFORM GmbH, Version 4, Stand November 2019

1 Maßnahmen zu Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

Zutrittskontrolle **Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.**	**vorhanden** **ja**
Elektronische Zutrittscodekarten/ Zutrittstransponder	x
Zutrittsberechtigungskonzept	x
Videoüberwachung	x
Alarmanlage	x
Schlüsselregelung	x
Begleitung von Besucherzutritten durch eigene Mitarbeiter	x
Sicherung auch außerhalb der Arbeitszeit durch Werkschutz	x
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	x
Gesicherter Eingang für An- und Ablieferung	x
Spezialverglasung (Erdgeschoß)	x
Aufbewahrung der Server in verschlossenen Räumen	x
Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen	x
Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe	x
Anweisung zur Ausgabe von Transponder	x

1.2 Zugangskontrolle

Zugangskontrolle **Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.**	**vorhanden** **ja**
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	x
Passwortsicherung von Bildschirmarbeitsplätzen	x
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	x
Verwendung von individuellen Passwörtern	x
Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	x
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	x
▪ Mindestens acht Ziffern	x
▪ Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. vier Kriterien)	x
▪ Wechsel des Passworts nach max. 180 Tagen	x
▪ Verhinderung von Trivialpasswörtern (z.B. Hund1, Hund2, Hund3)	x
▪ Passworthistorie (keine erneute Verwendung der letzten 10 Passwörter)	x
Hashing von gespeicherten Passwörtern	x
▪ SHA3	x
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	x
Teilw. Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	x
Teilw. Prozess zum Rechteentzug bei Austritt von Mitarbeitern	x
Verpflichtung auf Vertraulichkeit	x
Kontrollierte Vernichtung von Datenträgern	x
Aufbewahrung personenbezogener Daten in verschließbaren Sicherheitsschränken	x

1.3 Zugriffskontrolle

Zugriffskontrolle **Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.**	**vorhanden ja**
Festlegung der Zugriffsberechtigung, Berechtigungskonzept	x
Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung	x
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	x
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	x
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	x
Teilw. zeitliche Begrenzung von Zugriffsmöglichkeiten	x
Teilw. Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	x
Werden entsprechende Sicherheitssysteme (Software/Hardware) eingesetzt?	
▪ Virenscanner	x
▪ Firewalls	x
▪ SPAM-Filter	x
▪ Teilw. Intrusionprevention (IPS)	x
▪ Teilw. Intrusiondetection (IDS)	x
Teilw. verschlüsselte Speicherung der Daten	
▪ verwendete Verschlüsselungsalgorithmen:	
▫ AES (128/256 bit)	x
▫ 3DES	x
▫ RSA (1024/2048 bit)	x
▪ Verwendete Hash-Funktion:	
▫ SHA2 (256, 384, 512 bit)	x
▫ SHA3	x
▫ bcrypt	x

1.4 Auftragskontrolle

Auftragskontrolle **Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden.**	**vorhanden ja**
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)	x
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	x
Vorabkontrollen beim Auftragnehmer vor Vertragsbeginn	x
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)	x
Vor-Ort-Kontrollen beim Auftragnehmer	x
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer (sofern vorgelegt)	x
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer (sofern vorgelegt)	x
Erteilung von Weisungen zur Verbesserung des Datenschutzes ggü. Auftragnehmer	x

1.5 Trennungskontrolle

Trennungskontrolle **Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.**	**vorhanden ja**
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	x
Dateiseparierung bei Datenbanken	x
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	x
Verarbeitung der Daten des Auftraggebers u.a. Kunden v. untersch. Mitarbeitern d. Auftragnehmers	x
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	x
Funktionstrennung	x
Trennung von Entwicklungs-, Test- und Produktivsystem	x

2 Maßnahmen zur Gewährleistung der Integrität

2.1 Weitergabekontrolle

Weitergabekontrolle **Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.**	**vorhanden** **ja**
Welche Versendungsart der Daten besteht zwischen Auftraggeber und Dritten?	
▪ Citrix-Verbindung (128 Bit verschlüsselt)	x
▪ VPN-Verbindung (IP-Sec)	x
▪ E-Mail-Versand mit verschlüsselten ZIP-Dateien	x
▪ Datenaustausch über https-Verbindung	x
▫ verwendetes Verschlüsselungsprotokoll:	
- TLS 1.2	x
Gesicherter Eingang für An- und Ablieferung	x
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	x
Verschlüsselung vertraulicher Datenträger	x
Verschlüsselung von Laptopfestplatten	x
Verschlüsselung mobiler Datenträger	x
Kontrollierte Vernichtung von Daten	x
Datenträgerentsorgung - Sichere Löschung von Datenträgern:	
▪ Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	x
Papierentsorgung: Sicheres Vernichten von Papierdokumenten:	
▪ Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	x
▪ Shredder gem. DIN 66399	x

2.2 Eingabekontrolle

Eingabekontrolle **Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten**	**vorhanden** **ja**
Festlegung von Benutzerberechtigungen (Profile)	x
Lesen, Ändern, Löschen	x
Teilzugriff auf Daten bzw. Funktionen	x
Feldzugriff bei Datenbanken	x
Teilw. organisatorische Festlegung von Eingabezuständigkeiten	x
Protokollierung von Eingaben/Löschungen	x
Verpflichtung auf das Datengeheimnis	x
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	x

3 Maßnahmen zur Gewährleistung der Verfügbarkeit

3.1 Verfügbarkeitskontrolle

Verfügbarkeitskontrolle **Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.**	**vorhanden** **ja**
Datensicherungs- und Backupkonzepte	x
Durchführung der Datensicherungs- und Backupkonzepte	x
Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal	x

Brandmeldeanlagen in Serverräumlichkeiten	x
Rauchmelder in Serverräumlichkeiten	x
Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten	x
Klimatisierte Serverräumlichkeiten	x
Blitz-/ Überspannungsschutz	x
Wassersensoren in Serverräumlichkeiten	x
Serverräumlichkeiten in separaten Brandabschnitt	x
Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt	x
Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft	x
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	x
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten	x
Aufbewahrung der Daten in Datensicherungsschränken, Tresoren	x
USV-Anlage (Unterbrechungsfreie Stromversorgung)	x

4 Maßnahmen zur Gewährleistung der Belastbarkeit

4.1 Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle **Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.**	**vorhanden ja**
Redundante Stromversorgung	x
Redundante Datenanbindung	x
Redundante Klimatisierung	x
Redundante Brandbekämpfung	x
Festplattenspiegelung	x
Einsatz einer hochverfügbaren SAN-Lösung	x
Loadbalancer	x
Datenspeicherung auf RAID-Systemen (RAID 1 und höher)	x
Abgrenzung kritischer Komponenten	x
Teilw. Durchführung von Penetrationstests (für Anwendungs- und Entwicklungssysteme)	x
Teilw. Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	x
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	
▪ Identifikation der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Bestimmung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen.	x
▪ Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden.	x
▪ Definition von Zeiträumen, in denen die Updates implementiert werden sollen (z. B. Perioden niedrigerer Operationen, Wartungszeiten usw.).	x
▪ Teilw. Verwendung redundanter Systeme, um den Betrieb aufrecht zu erhalten, während die Hauptgeräte aktualisiert werden.	x
▪ Progressive Bereitstellung von Updates / Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen.	x
▪ Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen.	x
Sicherheit wird während der Entwurfsphase der Systeme als Hauptbetrachtung mit umfasst.	
▪ Definition von Sicherheitsmaßnahmen zum Schutz und zur Validierung der Kommunikation zwischen Systemkomponenten	x
▪ Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit.	x
▪ Widerruf vorübergehender Privilegien, sobald sie nicht mehr erforderlich sind.	x

▪ Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.	x
▪ Bei der Definition von Netzwerkkommunikationstechnologien und Architektur wird auch die Interoperabilität mit einbezogen.	x
▪ Identifizierung von Systemen, Infrastrukturen und Umgebungen, die eine Interkommunikation mit anderen Systemen (intern oder extern) erfordern, oder die diese Interkommunikation in naher Zukunft erfordern (unter Berücksichtigung des Lebenszyklus der beteiligten Geräte).	x
▪ Auswahl von Kommunikations-Protokollen, die mit den identifizierten Systemen und den Systemen der anderen Organisationen oder Umgebungen kompatibel sind.	x
▪ Kollaborative Umgebungen, die den Austausch von Informationen zwischen verschiedenen Parteien ermöglichen.	x
▪ Identifizierung und Austausch in einer gemeinsamen Plattform über potentielle Hauptangriffsvektoren.	x
Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation.	
▪ Sensibilisierungskampagnen, um die Benutzer über die Sicherheitskonzepte zu informieren, die sowohl für konkrete Systeme als auch für traditionelle IT-Systeme spezifisch sind.	x
▪ Spezielles Sicherheitstraining, um zu lehren, wie man Sicherheitsmaßnahmen und Verhaltensweisen auf die täglichen Prozesse mit möglichst geringem Aufwand anwendet.	x
▪ Triptychons, die vor neuen Bedrohungen und Risiken warnen, sowie als Erinnerung an die gemeinsamen Sicherheitspraktiken und -funktionen (ähnlich wie bei traditionellen Arbeitsplatz-Triptychonen) dienen.	x

5 Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren

Kontrollverfahren **Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren**	**vorhanden ja**
Verarbeitungsverzeichnisse werden mind. jährlich aktualisiert	x
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	x
Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten	x
Es werden datenschutzfreundliche Voreinstellungen gewählt	x
Getroffene Sicherheitsmaßnahmen werden teilw. einer regelmäßigen internen Kontrolle unterzogen	x
Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt	x