Auftragsverarbeitungsvertrag für die Überlassung von Standardsoftware und Supportleistungen

zwischen

dem in der Einzelvereinbarung definierten Kunden

– nachfolgend „**Verantwortlicher**“ oder „**Auftraggeber**“ genannt –

und

LWsystems GmbH & Co. KG, Tegelerweg 11, 49186 Bad Iburg

– nachfolgend „**Auftragnehmer**“ genannt –

gemeinsam "**die Parteien**"

Präambel

Der Auftragnehmer erbringt dem Verantwortlichen Standardsoftware und Supportleistungen nach Maßgabe der AGB Softwareüberlassung, sämtlichen Annexe und der Einzelvereinbarung (im Folgenden "**Hauptvertrag**"). In diesem Zusammenhang wird der Auftragnehmer mit personenbezogenen Daten des Verantwortlichen in Berührung kommen. Mit diesem Auftragsverarbeitungsvertrag (im Folgenden „**AVV**“) werden die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der Erbringung von dem in dem vorgenannten Vertrag geregelten Leistungsumfang durch den Auftragsverarbeiter ergeben, festgehalten.

1. Gegenstand und Dauer der Verarbeitung

a. Der Auftragnehmer erbringt die Dienstleistungen auf der Grundlage des zwischen den Parteien geschlossenen Hauptvertrags.

b. Einzelheiten über die Verarbeitung personenbezogener Daten im Rahmen des Vertrags, einschließlich der Arten der verarbeiteten personenbezogenen Daten und der Kategorien der betroffenen Personen, sind in Anlage 1 dieser AVV festgelegt.

c. Die Laufzeit dieser Vereinbarung sowie ihre Kündigungsfristen richten sich nach den Bestimmungen des Hauptvertrags, vorausgesetzt, dass sich aus den Bestimmungen dieser Vereinbarung keine weitergehenden Verpflichtungen ergeben. Aufgrund der Abhängigkeit vom Hauptvertrag endet diese Vereinbarung mit der Beendigung des Hauptvertrags. Das Recht zur außerordentlichen Kündigung dieser Vereinbarung bleibt davon unberührt. Im Falle des Fehlens von Bestimmungen zur Vertragsdauer und Kündigung im Hauptvertrag endet diese Vereinbarung mit der Erfüllung der zwischen den Parteien vereinbarten Verarbeitungstätigkeiten.

2. Ort der Verarbeitung

a. Die Verarbeitung personenbezogener Daten für die Zwecke des Hauptvertrages erfolgt grundsätzlich in Deutschland. Wenn die Verarbeitung personenbezogener Daten im Einzelfall nach Maßgabe eines Hauptvertrages für die Zwecke des Hauptvertrages in Ländern außerhalb der EU oder des EWR erfolgt, wird die Angemessenheit des Datenschutzniveaus gemäß den Bestimmungen von Art. 44 ff. DSGVO sichergestellt.

b. Mit der Unterzeichnung des Hauptvertrags gibt der Verantwortliche seine Zustimmung zur Datenverarbeitung gemäß Anlage 1 dieses AVV, einschließlich – sofern im Einzelfall vorgesehen und in Anlage 1 oder einer dokumentierten Weisung oder Vertragsänderung festgehalten – der Verarbeitung von Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums und des Zugriffs auf Daten von außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums.

3. Rechte und Pflichten des Auftraggebers

a. Im Rahmen dieses AVV ist der Auftraggeber Verantwortlicher im Sinne von Art. 4 Ziff. 7 DSGVO und insbesondere verantwortlich für die Rechtmäßigkeit der Datenübermittlung an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung.

b. Mit Unterzeichnung des Hauptvertrags erteilt der Auftraggeber die Weisung, personenbezogene Daten auftragsgemäß wie in der Leistungsvereinbarung beschrieben zu verarbeiten. Bei Bedarf kann der Auftraggeber darüber hinaus in schriftlicher oder einer anderen dokumentierten Form Einzelweisungen erteilen. Änderungen des Verarbeitungsgegenstands und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Dies gilt nicht für Änderungen des Hauptvertrags. Diese sind zwischen dem Auftragnehmer und dem Auftrag-

geber nach den Bestimmungen des Hauptvertrags zu vereinbaren.

c. Der Auftraggeber informiert den Auftragnehmer unverzüglich über alle bei der Ausführung der vereinbarten Leistung festgestellten Fehler und Störungen.

4. Rechte und Pflichten des Auftragnehmers

a. Der Auftragnehmer wird die im Geltungsbereich dieses Auftragsverarbeitungsvertrags verarbeiteten personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers verarbeiten, es sei denn es liegt eine entgegenstehende rechtliche Verpflichtung des Auftragnehmers vor. Der Auftraggeber bevollmächtigt den Auftragsverarbeiter zur Erstellung aggregierter nicht-personenbezogener Daten sowie zur Erstellung von Statistiken im Zusammenhang mit Kundendaten für die Abrechnungszwecke, Financial Reporting sowie zur Fortentwicklung der Standardsoftware.

b. Der Auftragnehmer beschränkt den Zugang zu personenbezogenen Daten innerhalb seiner Organisation auf Mitarbeiter, die zur Erbringung der Leistungen im Rahmen des Hauptvertrags Zugang zu den personenbezogenen Daten benötigen und zur Vertraulichkeit verpflichtet sind, und die zuvor mit den für sie relevanten Datenschutzbestimmungen vertraut gemacht wurden.

c. Der Auftragnehmer hat den Auftraggeber unverzüglich in Textform zu informieren, wenn er der Ansicht ist, dass eine Weisung gegen deutsche oder europäische Datenschutzvorschriften verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wird.

d. Unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung seiner Verpflichtungen hinsichtlich der Sicherheit der Verarbeitung. Darüber hinaus unterstützt der Auftragnehmer den Auftraggeber in angemessenem Umfang bei der Benachrichtigung der Aufsichtsbehörden und der betroffenen Personen im Fall von Verletzungen des Schutzes personenbezogener Daten, bei der Datenschutzfolgenabschätzung und im Falle einer möglichen Konsultation einer Aufsichtsbehörde.

e. Soweit sich betroffene Personen mit einem Ersuchen mit Bezug auf Pflichten des Auftraggebers unmittelbar an den Auftragnehmer wenden, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Abhängig von der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Betroffenenanfragen.

f. Der Auftragnehmer wird den Auftraggeber auf dessen Nachfrage in angemessener Weise mit geeigneten technischen und organisatorischen Maßnahmen für die Bearbeitung von Betroffenenanfragen nach anwendbarem Datenschutzrecht (einschließlich des Rechts auf Berichtigung oder Löschung personenbezogener Daten) unterstützen.

g. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung seiner Verpflichtungen gemäß Artikel 32 bis 36 DSGVO.

5. Sicherheit der Verarbeitung

a. Der Auftragnehmer wird angemessene technische und organisatorische Maßnahmen im Sinne von Art. 32 DSGVO zum Schutz der personenbezogenen Daten vor unbefugter Verarbeitung (einschließlich unbefugter Offenlegung, unbefugtem Zugriff, Verlust, Änderung und Zerstörung) ergreifen. Dabei sind (i) der Stand der Technik, (ii) die Kosten der Umsetzung, (iii) die Art der verarbeiteten personenbezogenen Daten und (iv) die Risiken für die betroffenen Personen zu berücksichtigen.

b. Die technischen und organisatorischen Maßnahmen, die in Anhang 2 dieser Vereinbarung dargelegt sind, werden vom Auftraggeber als geeignet für die Datenverarbeitung im Rahmen des Auftrags betrachtet und bilden einen integralen Bestandteil dieser Vereinbarung.

c. Dem Auftragnehmer ist gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in Anhang 2 festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6. Unterauftragsverhältnisse (weitere Auftragsverarbeiter)

a. In Anlage 3 dieses AVV sind alle weiteren Auftragsverarbeiter aufgeführt, die zum Zeitpunkt des Vertragsabschlusses vom Auftragnehmer im Rahmen des Hauptvertrags beschäftigt werden und personenbezogene Daten des Auftraggebers verarbeiten (im Folgenden "Unterauftragnehmer"). Mit Unterschrift dieser Vereinbarung genehmigt der Auftraggeber den Einsatz der in Anlage 3 genannten Unterauftragnehmer und aller künftigen zusätzlichen Unterauftragnehmer. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleis-

tungen, Standard-IT-Dienste (wie Hosting-Dienste), Wartungs- und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

b. Der Auftragnehmer teilt dem Auftraggeber beabsichtigte Änderungen in Bezug auf den Einsatz der in Anlage 3 genannten Unterauftragnehmer mit, einschließlich der Verwendung neuer Unterauftragnehmer.

c. Der Auftraggeber kann gegen die beabsichtigten Änderungen innerhalb von zwei (2) Wochen nach Information des Auftragnehmers über die geplanten Änderungen Widerspruch einlegen. Sofern der Auftraggeber binnen dieser Frist keinen Widerspruch einlegt, gelten die geplanten Änderungen des Auftragnehmers als genehmigt. Widerspricht der Auftraggeber den Änderungen, ist der Auftragnehmer berechtigt, den Hauptvertrag einschließlich dieser Vereinbarung zur Auftragsverarbeitung fristlos zu kündigen oder eine angemessene Vergütung für die durch den Widerspruch entstandenen Aufwendungen zu verlangen.

d. Im Falle des Einsatzes eines Unterauftragnehmers schließt der Auftragnehmer mit diesem einen dokumentierten Vertrag über die Verarbeitung personenbezogener Daten ab. In diesem Vertrag wird der Auftragnehmer dem Unterauftragnehmer Verpflichtungen auferlegen, die den Verpflichtungen in dieser Vereinbarung im Wesentlichen gleichwertig sind.

7. Kontrollrechte des Auftraggebers

a. Zum Nachweis der in Anlage 2 dieser Vereinbarung festgelegten technischen und organisatorischen Sicherheitsmaßnahmen wird der Auftragnehmer auf Anfrage des Auftraggebers aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit vorlegen.

b. Der Auftraggeber kann in den folgenden Fällen Vor-Ort-Audits beim Auftragnehmer durchführen, wenn und soweit dem keine rechtlichen Verpflichtungen des Auftragnehmers, insbesondere datenschutzrechtliche oder Vertraulichkeitsverpflichtungen, entgegenstehen, (i) wenn und soweit der Auftraggeber andernfalls seine gesetzlichen Verpflichtungen nicht erfüllen kann; oder (ii) wenn und soweit eine Datenschutzbehörde den Auftraggeber rechtlich bindend zu einer

Vor-Ort-Kontrolle verpflichtet; und soweit es technisch sichergestellt werden kann, dass während eines Audits kein Zugriff auf Daten, die nicht im Rahmen des Vertrags mit dem Auftraggeber verarbeitet werden, und insbesondere auf Daten anderer Kunden des Auftragnehmers, erfolgen kann.

c. Die Durchführung von Audits und Inspektionen ist auf maximal ein Audit oder eine Inspektion pro Kalenderjahr beschränkt. Abweichend hiervon ist die Durchführung von Audits und Inspektionen aufgrund einer durch eine Datenschutzbehörde auferlegten Verpflichtung oder aufgrund eines gesetzlich häufiger angeordneten Überprüfungszyklus, auch häufiger als einmal pro Kalenderjahr möglich.

d. Der Auftragnehmer ist berechtigt, eine angemessene Vergütung für die Unterstützung des Auftraggebers während eines Audits oder einer Inspektion zu verlangen, es sei denn, im Rahmen des Audit wird ein Verstoß des Auftragnehmers gegen die Bestimmungen dieses AVV festgestellt.

e. Der Umfang der Überprüfung und Kontrolle ist auf die Verarbeitung der personenbezogenen Daten des Auftraggebers im Rahmen der vereinbarten Leistungserbringung durch den Auftragnehmer beschränkt.

f. Audits sind rechtzeitig, mindestens jedoch zwei Wochen vor dem Audit, anzukündigen und während der üblichen Geschäftszeiten des Auftragnehmers durchzuführen, sofern gesetzliche Bestimmungen dem nicht entgegenstehen.

g. Der Auftragnehmer kann die Vorlage von Informationen oder den Zugang zu Geschäftsräumen und IT-Systemen verweigern, wenn und soweit dies gegen Vertraulichkeitsverpflichtungen des Auftragnehmers verstoßen könnte.

h. Inspektionen und Audits dürfen nur von Prüfern vorgenommen werden, die nicht im Wettbewerb zum Auftragnehmer stehen.

i. Der Auftraggeber verpflichtet sich, die ihm im Rahmen eines Audits oder einer Inspektion zur Kenntnis gelangten Nachweise, Auditberichte oder Berichtsauszüge sowie Testate und Zertifizierungen sowie sonstige Informationen vertraulich zu behandeln und nicht an Dritte weiterzugeben, es sei denn, der Auftraggeber ist hierzu gesetzlich oder aufgrund einer rechtsverbindlichen behördlichen Anordnung verpflichtet. Sämtliche Nachweise, Auditberichte, Berichtsauszüge, Testate und Zertifizierungen sowie sonstigen Informationen werden vom Auftraggeber ausschließlich zum Zweck der Überprüfung der Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen verwendet.

8. Benachrichtigungen bei Datenschutzverstößen

Der Auftragnehmer hat den Auftraggeber unverzüglich zu benachrichtigen, wenn er von einer zufälligen oder unbefugten Zerstörung, einem Verlust, einer Änderung, einer Offenlegung oder einem unbefugten Zugriff auf personenbezogene Daten (einschließlich der von einem Unterauftragnehmer verarbeiteten
personenbezogenen Daten) Kenntnis erhält, und er hat unverzüglich Maßnahmen zu ergreifen, um die der unbefugten Verarbeitung zugrunde liegenden Ursachen zu beseitigen und eine Wiederholung zu verhindern.

9. Löschen von personenbezogenen Daten nach Beendigung des Hauptvertrages

a. Nach Beendigung des Auftrags wird der Auftragnehmer die diesem Auftrag unterfallenden und im Besitz oder unter der Kontrolle des Auftragnehmers verbliebenen personenbezogenen Daten des Auftraggebers löschen oder an den Auftraggeber zurückgeben.

b. Eine Datenlöschung und -vernichtung unterbleibt soweit und solange der Auftragnehmer aufgrund gesetzlicher Vorgaben oder behördlicher Anordnung zur Aufbewahrung verpflichtet ist, oder im Ausnahmefall ein berechtigtes Eigeninteresse an der Aufbewahrung der Daten hat.

10. Schlussbestimmungen

a. Im Übrigen finden auf diese Vereinbarung die Bestimmungen des Hauptvertrags Anwendung, insbesondere im Hinblick auf die Regelung zum anwendbaren Recht und die Haftung des Auftragnehmers.

b. Im Fall eines Widerspruchs im Hinblick auf Regelungen für die Verarbeitung von personenbezogenen Daten zwischen Regelungen des Hauptvertrags sowie sonstigen zwischen Auftragnehmer und Auftraggeber geschlossenen Vereinbarungen zu der vertragsgegenständlichen Leistung und dieser Vereinbarung zur Auftragsverarbeitung, haben die Regelungen dieses AVV Vorrang.

Anlagen:

Anlage 1: Beschreibung der Datenverarbeitung

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Weitere Auftragsverarbeiter

Anlage 1: Beschreibung der Datenverarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden:	Kunden, Interessenten, Lieferanten, Partnern, öffentliche Stellen sowie andere Kommunikationspartner des Kunden sowie jeweils deren Mitarbeiter und Ansprechpartner
Kategorien der übermittelten personenbezogenen Daten:	Vom Kunden für die Erbringung von Supportleistungen übermittelte personenbezogene Daten; Kontaktdaten des Kunden-Ansprechpartners, der sich für die Erbringung von Supportleistungen an den Anbieter wendet
Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:	Übermittlung von sensiblen personenbezogenen Daten bei Support-Anfragen durch den Kunden untersagt.
Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden):	Kontinuierlich, bei Bedarf
Zweck(e) der Datenübermittlung und Weiterverarbeitung:	Erbringung von Supportleistungen und Professional Services i.R.d. Hauptvertrages
Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer:	Dauer des Hauptvertrages

Anlage 2: Technische und organisatorische Maßnahmen

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

- Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen, dokumentierte Schlüsselvergabe an Mitarbeiter)
- Zugangskontrolle (keine unbefugte Systembenutzung, Kennwort-/Passwortschutz zur Benutzeridentifikation und Authentifizierung an Workstations und Servern, Einrichtung eines Benutzerstammsatzes pro User, Zwei-Faktor-Authentisierung für Fernwartung von Kundensystemen (Zugang ist passwort- und zugriffsschlüsselgeschützt, Zugriff besteht nur für Mitarbeiter, verwendete Passwörter müssen Mindestlänge haben)
- Zugriffskontrolle (regelmäßige Sicherheitsupdates stellen sicher, dass unberechtigte Zugriffe verhindert werden, Berechtigungskonzept mit Zugriffsrechten, anwenderbezogene differenzierte Berechtigungen; je nach Benutzer mit Berechtigung zur Veränderung bzw. Löschung)
- Trennungskontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, mandantenfähige Software)
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO): Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

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

- Weitergabekontrolle
- kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport (alle Mitarbeiter sind auf das Datengeheimnis gemäß DSGVO verpflichtet, verschlüsselter Transport und verschlüsselte Übertragung bei sensitiven Daten, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur)
- Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust Spiegeln von Festplatten, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Spam-Filter, Firewall)
- Rasche Wiederherstellbarkeit (Serverspiegelung, Backups)

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

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle

Anlage 3: Weitere Auftragsverarbeiter

Der Verantwortliche hat bei der Inanspruchnahme keine Unterauftragsverarbeiter genehmigt.