

Auftragsverarbeitungs-Vereinbarung (AVV) EU- intern

[gemäß Standardvertragsklauseln nach EU-Durchführungsbeschluss EU 2021/915 Opt 1]

zwischen

Firma: **[FIRMA_AG]**
vertreten durch: **[Geschäftsführung]**
Straße: **[STRASSE+NR_AG]**
PLZ, Ort: **[PLZ_AG] [ORT_AG]**
Telefon:
E-Mail:

– im Folgenden „Auftraggeber“ oder „Verantwortlicher“ genannt –

und

Firma: **Extern Messdienst Süd GmbH & Co. KG**
vertreten durch: **Extern Messdienst Süd Verwaltungs-GmbH,
vertreten durch Albrecht Dern**
Straße: **Seckenheimer Straße 79**
PLZ, Ort: **68165 Mannheim**
Telefon:
E-Mail:

– im Folgenden „Auftragnehmer“ oder „Auftragsverarbeiter“ genannt –

ABSCHNITT I

Klausel 1 – Zweck und Anwendungsbereich

- a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Datenschutz-Grundverordnung (DSVGO) sichergestellt werden.
- b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der DSGVO oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
- c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- d) Die Anhänge I bis IV sind Bestandteil der Klauseln.
- e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der DSGVO oder der Verordnung (EU) 2018/1725 unterliegt.
- f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der DSGVO oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2 – Unabänderbarkeit der Klauseln

- a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
- b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 – Auslegung

- a) Werden in diesen Klauseln die in der DSGVO oder der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO oder der Verordnung (EU) 2018/1725 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der DSGVO oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 – Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – Kopplungsklausel

- a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
- b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
- c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6 – Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 – Pflichten der Parteien

7.1 Weisungen

- a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
- b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU)

2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

- a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
- b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Der Datenimporteur und — während der Datenübermittlung — auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffene Person gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

7.6 Dokumentation und Einhaltung der Klauseln

- a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DSGVO oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.
- d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- e) Die Parteien stellen den zuständigen Aufsichtsbehörden die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

- a) Der Auftragsverarbeiter darf **keinen seiner Verarbeitungsvorgänge**, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, **ohne vorherige gesonderte schriftliche Genehmigung** des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens **30 Tage** vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.
- b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der DSGVO oder der Verordnung (EU) 2018/1725 unterliegt.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen,

einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

- d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.
- e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

- a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DSGVO oder der Verordnung (EU) 2018/1725 im Einklang stehen.
- b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DSGVO sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der DSGVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 – Unterstützung des Verantwortlichen

- a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
- b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

- 1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
 - 2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
 - 3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
 - 4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 – Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der DSGVO oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
- b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der DSGVO oder in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

- 1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- 2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- 3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

- c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der DSGVO zu unterstützen.

ABSCHNITT III – Schlussbestimmungen

Klausel 10 – Verstöße gegen die Klauseln und Beendigung des Vertrags

- a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der DSGVO oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - 1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 - 2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der DSGVO oder der Verordnung (EU) 2018/1725 nicht erfüllt;
 - 3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der DSGVO oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.
- c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
- d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Klausel 11 – Individuelle Vertragsbedingungen

Es gelten die Standardvertragsklauseln gemäß [Durchführungsbeschluss EU 2021/915](#) EU-Kommission ohne Abstriche und gehen allen Vereinbarungen vor. Etwaige sprachlichen Abweichungen in diesem Vertrag, dienen nur der einfacheren Verständlichkeit oder sind Druckfehler und dürfen nicht abweichend ausgelegt werden.

ANHANG I – LISTE DER PARTEIEN

Verantwortlicher

1. Verantwortlicher ist der Auftraggeber auf Seite 1 dieses Vertrags.

[Name der Kontaktperson]

[Funktion der Kontaktperson]

[Kontaktdaten der Kontaktperson]

Datum und Unterschrift: _____

2. [weiterer Verantwortlicher]

Datum und Unterschrift: _____

Auftragsverarbeiter

1. Auftragsverarbeiter ist der Auftragnehmer auf Seite 1 dieses Vertrags.

Kontaktperson:

Markus Vatter, Datenschutzbeauftragter

bbg bitbase group GmbH, Der Datenschutzbeauftragte, Am Heilbrunnen 47, D-72766

Reutlingen

Datum und Unterschrift: _____

ANHANG II - Beschreibung der Verarbeitung

1. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Kunden, Kunden von Kunden, Mitarbeiter, Mieter, Nutzer, Unterauftragsverarbeiter, Dienstleister des Kunden des Auftragsverarbeiters, Handelsvertreter, Ansprechpartner

2. Kategorien personenbezogener Daten, die verarbeitet werden

Stammdaten, Kommunikationsdaten (z.B. Telefon, E-Post), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Messdaten (wie Heizung, Warmwasser, Kaltwasser, Strom), Abrechnungsdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten

3. Verarbeitete sensible Daten

Es werden keine sensiblen Daten verarbeitet.

5. Art und Zweck der Verarbeitung

Vertragszweck ist die Erfassung, Dokumentation, Abrechnung und Übermittlung von Verbräuchen für Wärme, Wasser etc. für Sie und Ihre Kunden gemäß dem Hauptvertrag, unseren [AGB](#) und der [Leistungsbeschreibung](#).

Achtung: Unsere Leistung hängt – vor allem im Fall einer Funkmessung – wesentlich von Ihrer Mitarbeit ab. Wenn Mieter oder andere Nutzer wechseln, müssen Sie uns die Nutzungsbeendigung unverzüglich (in der Regel über die Softwareschnittstelle) mitteilen. Sonst besteht die Gefahr, dass die Vornutzer den Verbrauch ihrer Nachfolger erfahren können, was eine Datenpanne im Sinne der DSGVO zur Folge hätte. Das kann zu Meldepflichten nach [Artt. 33 f. DSGVO](#) und Schadenersatzpflichten führen.

6. Häufigkeit und Dauer der Verarbeitung

Die Kriterien für die Festlegung der Häufigkeit und Dauer ergeben sich aus dem Hauptvertrag.

ANHANG III – Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten

Technische Maßnahmen

- Anonymisierung von Daten
- Verschlüsselung von Datenträgern
- Verschlüsselung mobiler Geräte
- Verschlüsselung von Webseiten (SSL)
- Verschlüsselung von Datenbanken
- E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)
- Verschlüsselung von Passwörtern und Schlüsseln

2. fortdauernde Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

2.1 Zutrittsbeschränkungen

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"><input checked="" type="checkbox"/> Manuelle Schließsysteme<input checked="" type="checkbox"/> Sicherheitsschlösser<input checked="" type="checkbox"/> Videoüberwachung	<ul style="list-style-type: none"><input checked="" type="checkbox"/> Schlüsselregelung / Schlüsselliste<input checked="" type="checkbox"/> Besucher in Begleitung von Mitarbeiter<input checked="" type="checkbox"/> Abgestufte Sicherheitsbereiche und kontrollierter Zutritt<input checked="" type="checkbox"/> Gesondert gesicherter Zutritt zum Rechenzentrum<input checked="" type="checkbox"/> Aufbewahrung der Server in verschlossenen Räumen<input checked="" type="checkbox"/> Sorgfalt bei Auswahl des Reinigungspersonals

2.2 Zugangsbeschränkungen

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"><input checked="" type="checkbox"/> Anmeldung mit Benutzername und Passwort<input checked="" type="checkbox"/> Anmeldung mit biometrischen Daten<input checked="" type="checkbox"/> Anti-Viren-Software (Zentral)	<ul style="list-style-type: none"><input checked="" type="checkbox"/> Verwaltung von Benutzerberechtigungen<input checked="" type="checkbox"/> Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Anti-Viren-Software (Mobile Geräte) <input checked="" type="checkbox"/> Intrusion-Detection-Systeme <input checked="" type="checkbox"/> Firewall <input checked="" type="checkbox"/> VPN-Einsatz	<input checked="" type="checkbox"/> Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern <input checked="" type="checkbox"/> Prozess zum Rechteentzug bei Abteilungswechsel von Mitarbeitern <input checked="" type="checkbox"/> Prozess zum Rechteentzug bei Austritt von Mitarbeitern <input checked="" type="checkbox"/> Richtlinie „Sicheres Passwort“ <input checked="" type="checkbox"/> Richtlinie Firewall <input checked="" type="checkbox"/> Clean-Desk-Policy <input checked="" type="checkbox"/> Richtlinie „Desktopsperre“ <input checked="" type="checkbox"/> Passwortsicherung von Bildschirmarbeitsplätzen <input checked="" type="checkbox"/> Verpflichtung zur Vertraulichkeit

2.3 Zugriffsbeschränkungen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Verwaltung von Benutzerrechten an zentraler Stelle (Administrator)	<input checked="" type="checkbox"/> Berechtigungskonzept <input checked="" type="checkbox"/> Protokollierung von Dateizugriffen und -lösungen <input checked="" type="checkbox"/> Reduzierung der Anzahl der Administratoren <input checked="" type="checkbox"/> Passwortrichtlinien

3. Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Einsatz von USV-Systemen <input checked="" type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten <input checked="" type="checkbox"/> RAID System / Festplattenspiegelung <input checked="" type="checkbox"/> Regelmäßige Backups des gesamten Systems	<input checked="" type="checkbox"/> Kontrolle des Sicherungsvorgangs <input checked="" type="checkbox"/> Hardware-Support- und Serviceverträge <input checked="" type="checkbox"/> Regelmäßige Tests zur Datenwiederherstellung <input checked="" type="checkbox"/> Regelmäßige Schulung des IT-Personals

<input checked="" type="checkbox"/> Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft	
--	--

4. Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Regelmäßige Überprüfung der IT-Prozesse
<input checked="" type="checkbox"/> Interne Kontrollen
<input checked="" type="checkbox"/> Prüfung durch Berechtigungskonzept
<input checked="" type="checkbox"/> Funktionstrennung
<input checked="" type="checkbox"/> Regelmäßige Audits (z.B. durch den DSB)
<input checked="" type="checkbox"/> TOM-Audit durch den DSB
<input checked="" type="checkbox"/> Regelmäßige Überprüfung der Verfahren
<input checked="" type="checkbox"/> Durchführung von Folgenabschätzungen
<input checked="" type="checkbox"/> Check Technikgestaltung / Voreinstellungen
<input checked="" type="checkbox"/> Datenschutzmanagementsystems (DPMS) / Datenschutzhandbuch

5. Identifizierung und Autorisierung der Nutzer

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Zwei-Faktor-Authentifizierung	<input checked="" type="checkbox"/> Berechtigungskonzept
<input checked="" type="checkbox"/> Benutzerprofile	<input checked="" type="checkbox"/> Regelmäßige Prüfung von Berechtigungen
<input checked="" type="checkbox"/> Unterscheidung zwischen Berechtigungen	<input checked="" type="checkbox"/> Identifikation von neuen Mitarbeitern
<input checked="" type="checkbox"/> Auth. mit Benutzername / Passwort	<input checked="" type="checkbox"/> Verwaltung der Rechte durch Administratoren
<input checked="" type="checkbox"/> Rollentrennung von Test- und Produktivsystem	
<input checked="" type="checkbox"/> Passwort-Richtlinie	

6. Datenschutz während der Übermittlung

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Verschlüsselung der Übertragung	<input checked="" type="checkbox"/> Dokumentation Datenempfänger

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"><input checked="" type="checkbox"/> Es werden sichere Log-in-Verfahren eingesetzt<input checked="" type="checkbox"/> Firewall<input checked="" type="checkbox"/> VPN<input checked="" type="checkbox"/> Protokollierungsmaßnahmen<input checked="" type="checkbox"/> Die Sicherheitsmaßnahmen entsprechen dem Stand der Technik	<ul style="list-style-type: none"><input checked="" type="checkbox"/> Verifizierung Identität Datenempfänger<input checked="" type="checkbox"/> Sorgfältige Auswahl Transportmittel

7. Datenschutz während der Speicherung

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"><input checked="" type="checkbox"/> Trennung von Produktiv- und Testumgebungen<input checked="" type="checkbox"/> Physikalische Trennung (System / Datenbank / Speicher)<input checked="" type="checkbox"/> Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantenummern)<input checked="" type="checkbox"/> Es werden sichere Log-in-Verfahren eingesetzt<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern<input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern<input checked="" type="checkbox"/> Datenklassifizierung<input checked="" type="checkbox"/> Mandantenfähigkeit bei relevanten Anwendungen<input checked="" type="checkbox"/> Datensätze sind mit Zweckattribute versehen<input checked="" type="checkbox"/> Zugriffsbeschränkung<input checked="" type="checkbox"/> Protokollierung von Aktionen und Ereignissen<input checked="" type="checkbox"/> Nutzung zertifizierter Cloud Systeme (Microsoft, Google, Amazon, sonstige)<input checked="" type="checkbox"/> Firewall<input checked="" type="checkbox"/> Überwachung von Systemen und Diensten	<ul style="list-style-type: none"><input checked="" type="checkbox"/> Erstellung eines Berechtigungskonzepts<input checked="" type="checkbox"/> Festlegung von Datenbankrechten<input checked="" type="checkbox"/> Alle Speicherorte der Daten sind bekannt<input checked="" type="checkbox"/> Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können

<input checked="" type="checkbox"/> Die Sicherheitsmaßnahmen entsprechen dem Stand der Technik	
--	--

8. Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Manuelle Schließsysteme <input checked="" type="checkbox"/> Sicherheitsschlösser <input checked="" type="checkbox"/> Abschließbare Server-Schränke <input checked="" type="checkbox"/> Keine sanitären Anschlüsse im Serverraum oder darüber <input checked="" type="checkbox"/> Sicherheitsschlösser <input checked="" type="checkbox"/> Überwachung Serverraum (Temperatur & Feuchtigkeit) <input checked="" type="checkbox"/> Serverraum klimatisiert <input checked="" type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input checked="" type="checkbox"/> Zutrittsberechtigungskonzept / Zutrittskontrollkonzept <input checked="" type="checkbox"/> Besucher: Nur in Begleitung von Mitarbeitern <input checked="" type="checkbox"/> Sorgfältige Auswahl des Reinigungspersonals <input checked="" type="checkbox"/> Schlüsselregelung / Schlüsselliste <input checked="" type="checkbox"/> Abgestufte Sicherheitsbereiche und kontrollierter Zutritt <input checked="" type="checkbox"/> Aufbewahrung der Server in verschlossenen Räumen <input checked="" type="checkbox"/> Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal

9. Gewährleistung der Protokollierung von Ereignissen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Automatisierte Protokollierung <input checked="" type="checkbox"/> Automatisierte Protokollierung auf Applikationsebene <input checked="" type="checkbox"/> Benachrichtigung mit Echtzeit-Alarm <input checked="" type="checkbox"/> Synchronisation der Systemzeit	<input checked="" type="checkbox"/> Ereignisberichte <input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)

10. Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Supportverträge mit Dritten <input checked="" type="checkbox"/> Vereinbarungen zu Outsourcing (SLA)

- Einbeziehung DSB bei Konfiguration
- Konfiguration durch Fachpersonal
- Begrenzung der Anzahl von Administratoren

11. Maßnahmen für die interne Verwaltung der IT und der IT-Sicherheit

Organisatorische Maßnahmen

- externer Datenschutzbeauftragter
- Es wird ein Datenschutz-Management-System betrieben
- Verarbeitungsverzeichnis
- Informationssicherheitsmanagementsystem (ISMS)
- Regelmäßige Compliance-Audits / Überprüfungen
- Schulung der Mitarbeiter zur Datensicherheit
- IT-Team mit klaren Rollen / Verantwortlichkeiten
- Risikobewertung und Maßnahmen zum Risikomanagement auf allen Stufen und Ebenen
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Interne Verarbeitungsverzeichnisse werden mind. jährlich aktualisiert
- Zentrale Erfassung vorhandener Auftragsverarbeiter (einheitliches Vertragsmanagement)

12. Maßnahmen zur Zertifizierung, Qualitätssicherung von Prozessen und Produkten

Organisatorische Maßnahmen

- Klarer Überblick über die für Produkte/Dienstleistungen/Prozesse geltenden Bestimmungen
- Regelmäßige interne und/oder externe Audits
- Zuweisung von Audit-Verantwortlichkeiten an zertifizierte Experten
- Regelmäßige Überprüfung auf neue Voraussetzungen und Erneuerung von Zertifikaten

13. Datenminimierung

Technische Maßnahmen

- Festlegung von Datenbankrechten

Organisatorische Maßnahmen

- Vermeidung von doppelten Daten

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Sperrung / Ausblenden von nicht benötigten Feldern in einem betriebswirtschaftlichen System	<input checked="" type="checkbox"/> Identifikation des Zwecks der Verarbeitung <input checked="" type="checkbox"/> Sichere Löschung der Daten nach Ablauf der Aufbewahrungsfrist <input checked="" type="checkbox"/> Klare Zuständigkeiten für Löschverfahren <input checked="" type="checkbox"/> Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke <input checked="" type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

14. Datenqualität

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Festlegung von Datenbankrechten <input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Datenquellen und deren Qualität werden regelmäßig geprüft <input checked="" type="checkbox"/> Die Datenerfasser sind bekannt <input checked="" type="checkbox"/> Die Bedeutung der Datenqualität für den Datenschutz ist bekannt

15. Gewährleistung einer begrenzten Vorratsdatenspeicherung

Organisatorische Maßnahmen
Nicht relevant

16. Rechenschaftspflicht

Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Die Maßnahmen im Datenschutz werden dokumentiert <input checked="" type="checkbox"/> Es wird ein Verzeichnis der Verarbeitungstätigkeiten geführt und regelmäßig (mind. jährlich) aktualisiert <input checked="" type="checkbox"/> Privacy by Design und Privacy by Default Grundsätze werden eingehalten <input checked="" type="checkbox"/> Meldepflichten gegenüber der Aufsichtsbehörde werden eingehalten <input checked="" type="checkbox"/> Datenschutz-Folgeabschätzungen

- Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)
- Abschluss von Standardvertragsklauseln
- Schulungen / Sensibilisierungen
- Datenschutz-Team
- Angemessene Richtlinien zum Datenschutz
- Rechtsgrundlage für alle Aktivitäten vorhanden
- Maßnahmen und Auditberichte sind dokumentiert
- Anfragen von Betroffenen werden beantwortet
- Sichere Datenlöschung
- Datenschutzerklärung dokumentiert

17. Datenübertragbarkeit und Gewährleistung der Löschung

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Die Daten liegen in einfachen Datenformaten (CSV) zur Verfügung <input checked="" type="checkbox"/> Die Datenübertragung erfolgt mit Sicherheitsmaßnahmen (Verschlüsselung) <input checked="" type="checkbox"/> Es werden Standardverfahren für den Datenaustausch eingesetzt (XML, JSON) <input checked="" type="checkbox"/> Digitale Löschung von Daten <input checked="" type="checkbox"/> Protokollierungen von Löschungen <input checked="" type="checkbox"/> Aktenvernichter (mind. Stufe 3, crosscut) <input checked="" type="checkbox"/> Physische Löschung von Datenträgern 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Es werden Verfahren eingesetzt, um die Übertragung an Unberechtigte Empfänger zu vermeiden <input checked="" type="checkbox"/> Vor einer Datenübertragung wird geprüft, ob kein Ausschlussgrund für die Daten Portabilität besteht <input checked="" type="checkbox"/> Klare Zuständigkeiten für Löschverfahren <input checked="" type="checkbox"/> Klare Regelung zu Aufbewahrungsfristen <input checked="" type="checkbox"/> DSB berät zu Speicherfristen <input checked="" type="checkbox"/> Datentrennung nach Aufbewahrungsfristen <input checked="" type="checkbox"/> Eingesetzte Drittanbieter für Vernichtung von Informationen sind geprüft

18. Datenübermittlung an (Unter-)Auftragsverarbeiter

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Sichere Datenlöschung gewährleistet <input checked="" type="checkbox"/> Sichere Datenträgervernichtung gewährleistet 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Standardvertragsklauseln (SCC) werden vereinbart und unterzeichnet <input checked="" type="checkbox"/> Vertraglich vereinbarte Kontrollen

Auftragsverarbeitungsvertrag EU-SVK intern nach DSGVO
[VERTRAG-ID]

Datum
27.02.2025

<p><input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten</p> <p><input checked="" type="checkbox"/> Protokollierung von Eingaben/Löschungen</p>	
---	--

ANHANG IV - Liste der Unterauftragsverarbeiter

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Name	Zwecke	Ort der Datenverarbeitung	Adresse
bbg bitbase group GmbH	Datenschutz und Datenschutzdokumentation	EU/EWG	Am Heilbrunnen 47 72766 Reutlingen
Sontex Deutschland GmbH	Zentrale Verbrauchsmessung per Funk	EU/EWG	Paul-Ehrlich-Straße 11 63322 Rödermark
Host Europe GmbH	Webbhosting	EU/EWG	c/o WeWork Wallarkaden Pilgrimstraße 6 50674 Köln