Vereinbarung zur Auftragsverarbeitung

auf Basis des Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021

Stand: Januar 2026

zwischen

Angaben zum Verantwortlichen

(nachfolgend Verantwortlicher genannt)

und

Kunze & Ritter GmbH
Christaweg 44
79114 Freiburg

(nachfolgend Auftragsverarbeiter genannt)

Präambel

Der vorliegende Vertrag basiert auf den Standarvertragsklauseln des Durchführungsbeschlusses (EU) 2021/915 der Kommission vom 4. Juni 2021 gemäß Artikel 28 Absatz 7 DSGVO und ist im Wortlaut mit Ausnahme dieser Präambel unverändert übernommen.

Diese Präambel dient der vereinfachten Prüfung durch Vertragspartner zur Klarstellung, dass dieser Vertrag die Mindestanforderungen der DSGVO erfüllt.

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 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) 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

Verordnung (EU) 2016/679 und/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 Verordnung (EU) 2016/679 und/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 Verordnung (EU) 2016/679 und/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 Verordnung (EU) 2016/679 bzw. 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 Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 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 – fakultativ

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

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

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 Verordnung (EU) 2016/679 und/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 der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens einen Monat im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

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 Verordnung (EU) 2016/679 und/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 Verordnung (EU) 2016/679 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 Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 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 Verordnung (EU) 2016/679 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 Verordnung (EU) 2016/679] 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 Verordnung (EU) 2016/679 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 Verordnung (EU) 2016/679 und/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 Verordnung (EU) 2016/679 und/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 Verordnung (EU) 2016/679 und/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.

ANHANG I

Liste der Parteien

Verantwortliche(r):

1. Name: Bitte Name angeben

   Anschrift: Bitte Anschrift angeben

   Name, Funktion und Kontaktdaten der Kontaktperson:

Unterschrift und Beitrittsdatum: 01.01.2026

Auftragsverarbeiter:

1. Name: Kunze & Ritter GmbH

   Anschrift: Christaweg 44, 79114 Freiburg

   Name, Funktion und Kontaktdaten der Kontaktperson:
   Emanuel Krupka, Geschäftsführer, 0761/455540, e.krupka@kunze-ritter.de
   Dietmar Ritter, Geschäftsführer, 0761/455540, d.ritter@kunze-ritter.de

Unterschrift und Beitrittsdatum: 01.01.2026

Externer Datenschutzbeauftragter:

Ingenieurbüro Bernd Hölle GmbH, Gerhard-Kindler-Straße 3, 72770 Reutlingen,

07121/8201740, kunze-ritter@ibh-datenschutz.de

ANHANG II

Beschreibung der Verarbeitung

A – Printing-Dienstleistungen

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Beschäftigte des Kunden (auch Bewerber, ehemalige Beschäftigte etc.)
- Geschäftspartner (Kunden, Lieferanten, Interessenten) des Kunden

Kategorien personenbezogener Daten, die verarbeitet werden können

- Personenstammdaten (z.B. Name, Geburtsdatum, Adresse, Zeiterfassung, Abteilung, Tätigkeit, Kostenstelle, Lohnabrechnungsdaten)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Leistungsdaten (z.B. aufgrund von Auswertungen)
- Protokollierungsdaten (Druck, Kopier, Scan- und Faxdaten, Benutzeranmeldungen)
- Logdaten des Multifunktionsgerätes

Art der Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber können folgendes umfassen.

- Installation von Multifunktionssystemen und Druckern beim Endkunden vor Ort
- Installation und Support von Printmanagementsoftware, Software zur Verwaltung der Multifunktionssysteme und Verbrauchsmaterialien
- Wartungsdienstleistungen an Multifunktionssystemen und Druckern (Beheben von Störungen, Supportleistungen, etc.)
- nach Vertragslaufzeit eventuelle Rücknahme der Altsysteme mit Verschrottung, dabei Ausbau, Löschung und Wiedereinbau der Festplatten innerhalb der Multifunktionssysteme und Drucker.

Zwecke, für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

- Bereitstellung von Druck-, Scan, Kopier- und Faxfunktionalitäten gemäß Dienstleistungsvertrag
- Support-Leistungen zur Sicherstellung der Funktionsfähigkeit während der Dauer des Vertrages.
- Bereitstellung von Verbrauchsmaterialien

Dauer der Verarbeitung

Die Daten werden nach Vertragsende gelöscht, sofern nicht aus Gewährleistungsgründen oder sonstigen gesetzlichen Vorschriften eine längere Verarbeitung notwendig ist.

B – IT-Dienstleistungen

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Beschäftigte des Kunden (auch Bewerber, ehemalige Beschäftigte etc.)
- Geschäftspartner (Kunden, Lieferanten, Interessenten) des Kunden

Kategorien personenbezogener Daten, die verarbeitet werden können

- Personenstammdaten (z.B. Name, Benutzername, Geburtsdatum, Adresse, Zeiterfassung, Abteilung, Tätigkeit, Kostenstelle, Lohnabrechnungsdaten)
- Active Directory Daten (Gruppenmitgliedschaften, Rollen, E-Mail-Adresse, Logon-Daten)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Leistungsdaten (z.B. aufgrund von Auswertungen)
- Protokollierungsdaten
- Daten aus Fachverfahren, auf die technisch bedingt Zugriff besteht (z.B. ERP, CRM, DMS, HR-System, etc.)

Art der Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber können folgendes umfassen:

- Fernwartung von Kundensystemen
- Patch-Management
- Monitoring von Systemzuständen
- Benutzerverwaltung
- Ticketsystem zur Bearbeitung von Supportanfragen

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

- IT-Serviceeinsätze
- Patch- und Änderungsmanagement
- Erhöhung der IT-Sicherheit (bei vorliegender Weisung)
- Einführung und Konfiguration von benötigter Soft- und Hardware
- Fehleranalyse
- Aufrechterhaltung des IT-Betriebs
- Vertragsgemäße Betreuung

Dauer der Verarbeitung

Die Daten werden nach Vertragsende gelöscht, sofern nicht aus Gewährleistungsgründen oder sonstigen gesetzlichen Vorschriften eine längere Verarbeitung notwendig ist.

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Beschreibung der von dem Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

VERTRAULICHKEIT

1. Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.

Technische Maßnahmen

- Gesicherte Gebäudezugänge mittels elektronischer Schließsysteme
- Protokollierung des Zutritts
- Türen mit Knauf Außenseite
- Zutritt zu Serverräumen und Sicherheitszonen nur für autorisierte Personen
- Alarmanlagen zur Gebäudesicherung an allen Standorten
- Brandschutz- und Klimatisierungskonzept für Serverräume
- Regelmäßige Wartung der sicherheitsrelevanten Anlagen (z. B. Einbruchmeldeanlagen, USV-Systeme)

Organisatorische Maßnahmen

- Besucherregelung mit Anmeldung und Begleitung
- Gebäudeeinlass nur nach Klingeln
- Sorgfalt bei der Auswahl der Reinigungsdienste
- Rollenbasierte Zutrittsberechtigungen

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen können.

Technische Maßnahmen

- Benutzerkennungen sind eindeutig und personenbezogen
- Verwendung starker Passwörter gemäß Passwortrichtlinie (mind. 10 Zeichen, Komplexitätsanforderung)
- Login mit biometrischen Daten
- Technische Erzwingung von Passwortanforderungen

- Zwei-Faktor-Authentifizierung für administrative Zugänge und Systeme mit hohem Risiko
- Automatische Sperrung von Endgeräten nach Inaktivität
- Verschlüsselter Fernzugriff (VPN, ZTNA) für Remote-Zugänge
- Firewall mit Regelwerk
- Verschlüsselung der Smartphones

Organisatorische Maßnahmen

- Richtlinie zur Nutzung mobiler Endgeräte
- Einsatz einer MDM-Lösung für mobile Endgeräte
- Zentrale Benutzerverwaltung
- regelmäßige Sensibilisierung zur Bildschirmsperre bei Verlassen des Arbeitsplatzes

3. Zugriffskontrolle

Maßnahmen, die sicherstellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen

- Akten-Schredder
- Physische Löschung von Datenträgern
- Trennung von Benutzer- und Administratorkonten
- Protokollierung von administrativen Tätigkeiten
- Einschränkung administrativer Rechte für normale Benutzer
- Zugriff auf personenbezogene Daten nur über autorisierte Anwendungen
- Verschlüsselung von Daten auf mobilen Geräten und Servern

Organisatorische Maßnahmen

- Rollen- und Berechtigungskonzept nach dem Need-to-know-Prinzip
- Regelmäßige Überprüfung und Anpassung von Berechtigungen

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Logische Trennung von Datenbeständen je nach Zweck und Verarbeitungstätigkeit
- Nutzung getrennter Systeme oder Datenbanken für unterschiedliche Mandanten und Anwendungen
- Berechtigungskonzepte verhindern unberechtigte Querverarbeitung
- Trennung von Entwicklungs-, Test- und Produktivsystemen
- Datensätze mit unterschiedlichen Aufbewahrungsfristen werden systematisch getrennt archiviert und gelöscht
- Netzwerksegmentierung

INTEGRITÄT

5. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen

- Verschlüsselung bei der Datenübertragung (TLS 1.2/1.3, HTTPS, VPN)
- Verschlüsselung mobiler Datenträger
- Nutzung sicherer Kommunikationskanäle (z. B. E-Mail mit Transport- oder Inhaltsverschlüsselung)
- Verwendung zertifizierter Cloud-Dienste mit AV-Verträgen
- Logging und Monitoring von Dateiübertragungen

6. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung von Benutzeraktivitäten in IT-Systemen
- Speicherung von Logdaten auf separatem, manipulationsgeschütztem Server
- Zeitstempelsynchronisation aller Systeme
- Regelmäßige Überprüfung der Logdaten auf sicherheitsrelevante Ereignisse

VERFÜGBARKEIT UND BELASTBARKEIT

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Notfall- und Wiederherstellungskonzepte (Business Continuity Management)
- Feuerlöscher Serverraum
- Serverraum klimatisiert
- Schutzsteckdosenleisten Serverraum
- RAID System / Festplattenspiegelung
- Tägliche Backups
- Schutz der Backups durch physische und logische Sicherheitsmaßnahmen
- USV-Systeme und Überspannungsschutz für Serverräume
- Regelmäßige Wartung und Monitoring kritischer Systeme

VERFAHREN zur regelmäßigen ÜBERPRÜFUNG, BEWERTUNG und EVALUIERUNG

8. Datenschutz-Maßnahmen

- Implementierung eines Datenschutz-Managementsystems
- Externer Datenschutzbeauftragter
- Regelmäßige Sensibilisierung der Mitarbeiter
- Bedarfsweise Durchführung einer Datenschutz-Folgenabschätzung
- Nachkommen der Informationspflichten nach Art. 13 und 14 DSGVO
- Führen eines Verzeichnisses für Verarbeitungstätigkeiten

9. Incident-Response-Management

- Spamfilter
- Virenscanner
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und Datenschutzverletzungen
- Dokumentation von Datenpannen
- Meldung von Vorfällen an Verantwortlichen unverzüglich, spätestens aber binnen max. 24h

10. Datenschutzfreundliche Voreinstellungen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Datenschutzfreundliche Konfiguration eingesetzter Lösungen (Privacy by default)
- Deaktivierung überflüssiger Dienste

11. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Abschluss von Auftragsverarbeitungsverträgen nach Art. 28 DSGVO bzw. EU Standardvertragsklauseln
- Auswahl von Dienstleistern nach Sicherheits- und Datenschutzkriterien (z. B. ISO 27001-Zertifizierung)
- Regelmäßige Überprüfung und Dokumentation der Dienstleister
- Verpflichtung der Dienstleister auf Vertraulichkeit
- Schriftliche Weisungen an den Auftragnehmer
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer

ANHANG IV

Liste der Unterauftragsverarbeiter

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Die Unterauftragsverarbeitung durch nachfolgend aufgeführte Unternehmen variiert je nach Auftrag und bedingt den Einsatz entsprechender Hard- und Softwarelösungen.

A – Printing-Dienstleistungen

Name	Standort	Leistung
TeamViewer Germany GmbH	Bahnhofsplatz 2 73033 Göppingen	Fernwartung
INFOMINDS AG	Brennerstraße 72, 39042 Brixen, (Italien)	Ticketsystem, Kundenportal
MPS Monitor S.r.l. (HP SDS Action Center)	Via Borromei 2, 20123 Mailand (Italien)	Flottenmanagement: Zählerstand, Firmware-Updates, Tonerstand
HP Deutschland GmbH	Herrenberger Straße 140 71034 Böblingen	3rd Level Support MFPs, Softwareanwendungen (HP Security Manager, Command Center Anwendungen)
dimatek GmbH	Peterzellerstr. 8 Gebäude B 78048 Villingen-Schwenningen	3rd Level Supportleistungen für Printmanagementlösungen PaperCut MF, PaperCut Hive
docuFORM GmbH	docuFORM GmbH Händelstr. 11 76185 Karlsruhe	Supportleistungen für Zählerstandssoftware
Konica Minolta Business Solutions Deutschland GmbH	Europaallee 17 30855 Langenhagen	3rd Level Support Multifunktionsgeräte, Document Navigator, SafeQ, Paragon, Fleet RMM, CS Remote Care (Production Printing Fleet Management), Marketplace Anwendungen
Lexmark Deutschland GmbH	Dornhofstraße 44 63263 Neu-Isenburg	3rd Level Support MFPs, Markvision, Appstore Anwendungen
MyQ Deutschland	Am Langen Weiher 5 Weisendorf, 91085	3rd Level Support Printmanagementlösungen MyQ, MyQ Roger
KYOCERA Document Solutions Deutschland GmbH	Otto-Hahn-Straße 12 40670 Meerbusch	Kyocera Fleet Services Hosting
OPTIMIDOC D/A/CH GmbH	Albert-Einstein-Ring 5 14532 Kleinmachnow	3rd Level Support der OptimiDoc Lösungen
stethos Systemhaus GmbH	Weimarer Str. 48	Einrichtung und Support W-

	D-71065 Sindelfingen	ELP Software
SCHWALENBERG Betriebs- und Datentechnik GmbH	Ilseder Hütte 10 31241 Ilsede	Support der Softwarelösung Cardpresso beim Einsatz von Kartendruckern
Tungsten Automation Deutschland GmbH	Engelbergerstrasse 19 79106 Freiburg im Breisgau	3rd Level Support und Cloud Hosting Printix Softwarelösung

B – IT-Dienstleistungen

Name	**Standort**	**Leistung**
TeamViewer Germany GmbH	Bahnhofsplatz 2 73033 Göppingen	Fernwartung
INFOMINDS AG	Brennerstraße 72, 39042 Brixen, (Italien)	Ticketsystem, Kundenportal
Sophos Ltd.	The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, UK	Hosting Sophos Central
HP Deutschland GmbH	Herrenberger Straße 140 71034 Böblingen	Carepack Services, WEX Plattform (Clienthardware)
Servereye GmbH	Koßmannstr. 7 66571 Eppelborn	Hosting Monitoring
Docuware GmbH	Planegger Str. 1 82110 Germering	3rd Level Support DocuWare Dokumentenmanagementsystem, Hosting beim Einsatz der Cloudlösung
Infinigate Deutschland GmbH	Richard-Reitzner-Allee 8 85540 Haar / München	3rd Level Support Sophos-Produkte
Wortmann AG	Bredenhop 20 32609 Hüllhorst	3rd Level Support Server, Terra Cloud Backup, 3rd Level Support M365 Tenants
AvePoint Deutschland GmbH	Nymphenburger Str. 3 80335 Munich,	Hosting M365-Backup
REDDOXX GmbH	Neue Weilheimer Str. 14 73230 Kirchheim	3rd Level Support E-Mail-Archivierung
ELOVADE Deutschland GmbH	Garbenheimer Str. 36 D-35578 Wetzlar	Cloud E-Mail-Archivierung Mailstore, Cloudspeicher Backup
REINER Kartengeräte GmbH und Co. KG	Baumannstr. 16-18 D-78120 Furtwangen	Zeiterfassung, 3rd Level Support
baramundi software GmbH	Forschungsallee 3 86159 Augsburg	3rd Level Support Endpoint Management
NETCONTROL GmbH	Waldstraße 32 D – 79206 Breisach a. Rh.	3rd Level Support K&R Archiv DMS-Lösung