AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

gemäß Art. 28 DSGVO

zwischen dem Kunden (Verantwortlicher) und der

iDWELL GmbH (Auftragsverarbeiter)

Geltungsbereich und Einbeziehung

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV") regelt die Auftragsverarbeitung personenbezogener Daten durch die iDWELL GmbH im Rahmen aller von der iDWELL GmbH angebotenen und vom Kunden gebuchten Software- und Service-Produkte.

Dieser AVV wird dem Kunden online bereitgestellt unter www.idwell.com/de/avv und wird durch ausdrückliche Bezugnahme im jeweiligen SaaS-Hauptvertrag (nachfolgend „Hauptvertrag") Vertragsbestandteil. Eine gesonderte Unterzeichnung dieses AVV ist **nicht erforderlich**; der Abschluss des Hauptvertrags durch den Kunden gilt zugleich als Annahme dieses AVV. Die Identität der Parteien ergibt sich jeweils aus dem Hauptvertrag.

Dokumenteninformation

Version	2.0
Stand	April 2026
Rechtsgrundlage	Art. 28 Abs. 3 und 4 DSGVO (Verordnung (EU) 2016/679)
Auftragsverarbeiter	iDWELL GmbH, Margaretenstraße 70/2/7, 1050 Wien, Österreich
Kontakt	kontakt@idwell.com | +49 89 997436845
Online-Bereitstellung	www.idwell.com/de/avv

ABSCHNITT I - ALLGEMEINE BESTIMMUNGEN

Klausel 1 - Zweck und Anwendungsbereich

A. Mit diesem AVV 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 - DSGVO) sichergestellt werden.

B. Der im Hauptvertrag als Kunde bezeichnete Vertragspartner („Verantwortlicher“) und die iDWELL GmbH („Auftragsverarbeiter“) haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 DSGVO zu gewährleisten.

C. Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

D. Die Anhänge I bis IV sind Bestandteil dieses AVV.

E. Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der DSGVO unterliegt.

F. Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V DSGVO erfüllt werden.

Klausel 2 - Verwendung der Klauseln

A. Diese Klauseln dürfen in einen umfangreicheren Vertrag aufgenommen werden und weitere Klauseln oder zusätzliche Garantien können hinzugefügt werden, 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 diesem AVV die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der DSGVO.

B. Dieser AVV ist im Lichte der Bestimmungen der DSGVO auszulegen.

C. Dieser AVV darf nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 - Vorrang

Im Falle eines Widerspruchs zwischen diesem AVV und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, hat dieser AVV Vorrang.

Klausel 5 - Kopplungsklausel

A. Eine Einrichtung, die nicht Partei dieses AVV ist, kann diesem AVV mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten. Der Beitritt erfolgt durch schriftliche Mitteilung an die iDWELL GmbH unter Angabe der im Hauptvertrag identifizierten Vertragsbeziehung; einer gesonderten Unterzeichnung der Anhänge bedarf es nicht.

B. Nach wirksamem Beitritt wird die beitretende Einrichtung als Partei dieses AVV behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend der im Beitrittsdokument vorgesehenen Bezeichnung.

C. Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesem AVV 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. Anhang II ist modular aufgebaut und differenziert zwischen den einzelnen iDWELL-Produkten; für den konkreten Verarbeitungsumfang sind ausschließlich die vom Kunden tatsächlich gebuchten Module im Sinne des Hauptvertrags maßgeblich.

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 DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

C. Als dokumentierte Weisungen gelten insbesondere der Hauptvertrag, die Produktkonfiguration des Verantwortlichen in der iDWELL-Plattform sowie nachweisbare Weisungen in Textform (z. B. per E-Mail oder über das Support-System).

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. Produkt- und modulspezifische Aufbewahrungsverpflichtungen - insbesondere handels- und steuerrechtliche Aufbewahrungsfristen für Rechnungen und Buchhaltungsunterlagen im Modul iDWELL Finance (siehe Anhang II Abschnitt C) - bleiben hiervon unberührt.

7.4 Sicherheit der Verarbeitung

A. Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen (TOM), 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 (nachfolgend „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.

C. Der Auftragsverarbeiter ist berechtigt, die TOM jederzeit weiterzuentwickeln, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten gemäß Art. 9 und Art. 10 DSGVO 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 (nachfolgend „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzliche Garantien an. Der Verantwortliche wird darauf hingewiesen, dass die iDWELL-Plattform nicht primär auf die Verarbeitung sensibler Daten ausgelegt ist; soweit solche Daten dennoch eingebracht werden (z. B. in Freitextfeldern, Anhängen oder Rechnungen von Gesundheitsdienstleistern), liegt die Rechtmäßigkeit der Verarbeitung ausschließlich im Verantwortungsbereich des Verantwortlichen.

7.6 Dokumentation und Einhaltung der Klauseln

A. Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können. Der Nachweis erfolgt durch den Auftragsverarbeiter mit angemessenem Aufwand und mit den ihm zur Verfügung stehenden Ressourcen nach bestem Bemühen.

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 hervorgehenden Pflichten erforderlich sind. Hierzu zählen insbesondere das aktuelle TOM-Dokument, Zertifizierungsnachweise (z. B. ISO/AWS) sowie Berichte über Penetrationstests in zusammengefasster Form.

D. Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

E. Der Verantwortliche ist berechtigt, die Einhaltung dieses AVV auch vor Ort durch Einsetzen eines unabhängigen, zur Verschwiegenheit verpflichteten Prüfers (der kein Wettbewerber des Auftragsverarbeiters sein darf), auf eigene Kosten, zu überprüfen; Inspektionen sind mit angemessener Vorlaufzeit (mindestens 30 Tage) anzukündigen, auf das erforderliche Maß zu beschränken und dürfen den Betrieb des Auftragsverarbeiters nicht unangemessen beeinträchtigen. Der Aufwand des Auftragsverarbeiters für Prüfungen, die über ein Mal pro Kalenderjahr hinausgehen, kann zu marktüblichen Sätzen in Rechnung gestellt werden.

7.7 Einsatz von Unterauftragsverarbeitern

A. Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in Anhang IV aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens zwei (2) Wochen im Voraus in Textform (z. B. per E-Mail oder In-App-Benachrichtigung) 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 DSGVO 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.

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 DSGVO 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 DSGVO beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V DSGVO sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 DSGVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

C. Die Hauptverarbeitung sämtlicher iDWELL-Produkte erfolgt innerhalb der Europäischen Union (AWS Region Frankfurt, Deutschland). Eine Übermittlung in Drittländer ist derzeit nicht vorgesehen; sollte sie im Einzelfall erforderlich werden, wird der Auftragsverarbeiter den Verantwortlichen vorab informieren und die Einhaltung von Kapitel V DSGVO sicherstellen.

Klausel 8 - Unterstützung des Verantwortlichen

A. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von einer 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 in angemessenem Rahmen den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte (Art. 12 bis 22 DSGVO) 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:

- Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO;
- Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) gemäß Art. 36 DSGVO;
- Verpflichtungen gemäß Art. 32 DSGVO (Sicherheit der Verarbeitung).

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 DSGVO 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:

- 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);
- bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 DSGVO in der Meldung des Verantwortlichen anzugeben sind und mindestens Folgendes umfassen müssen:
  - 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;
  - die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  - die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;
- bei der Einhaltung der Pflicht gemäß Artikel 34 DSGVO, 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.

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.

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, spätestens jedoch innerhalb von 48 Stunden, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- 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);
- Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

- 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 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 - 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 Hauptvertrag, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, zu kündigen, wenn:

- 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;
- der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der DSGVO nicht erfüllt;
- der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln oder der DSGVO zum Gegenstand hat, nicht nachkommt.

C. Der Auftragsverarbeiter ist berechtigt, den Hauptvertrag, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, zu kündigen, 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 (insbesondere handels- und steuerrechtliche Aufbewahrungspflichten im Modul iDWELL Finance). Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Klausel 11 - Aktualisierung und Änderung dieses AVV

A. Der Auftragsverarbeiter ist berechtigt, diesen AVV zu aktualisieren, um ihn an rechtliche, regulatorische oder technische Entwicklungen anzupassen, sofern das Schutzniveau für die betroffenen Personen nicht unterschritten wird.

B. Wesentliche Änderungen werden dem Verantwortlichen mindestens vier (4) Wochen vor Inkrafttreten in Textform (z. B. per E-Mail oder In-App-Benachrichtigung) mitgeteilt. Widerspricht der Verantwortliche der Änderung nicht innerhalb dieser Frist, gilt die aktualisierte Fassung als angenommen.

C. Im Falle eines fristgerechten Widerspruchs durch den Verantwortlichen bleiben die bisherigen Regelungen bis zur Klärung der Änderung in Kraft. Kann keine Einigung erzielt werden, sind beide Parteien berechtigt, den Hauptvertrag mit einer Frist von drei (3) Monaten zum Monatsende zu kündigen, soweit die Verarbeitung betroffen ist.

Klausel 12 - Haftung, Anwendbares Recht und Gerichtsstand

A. Die Haftung der Parteien bestimmt sich nach den Regelungen des Hauptvertrags sowie nach Art. 82 DSGVO. Eine im Hauptvertrag vereinbarte Haftungsbeschränkung gilt auch für Ansprüche aus oder im Zusammenhang mit diesem AVV, soweit dies gesetzlich zulässig ist.

B. Dieser AVV unterliegt dem materiellen Recht der Republik Österreich unter Ausschluss der Verweisungsnormen des Internationalen Privatrechts und unter Ausschluss des UN-Kaufrechts (CISG).

C. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist das für 1010 Wien sachlich zuständige Gericht, soweit dies gesetzlich zulässig ist. Zwingende gesetzliche Gerichtsstände, insbesondere zugunsten von Verbrauchern im Sinne des KSchG, bleiben unberührt.

Klausel 13 - Salvatorische Klausel

Sollten einzelne Bestimmungen dieses AVV ganz oder teilweise unwirksam oder undurchführbar sein oder werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der wirtschaftlichen und datenschutzrechtlichen Zielsetzung am nächsten kommen, die die Parteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Gleiches gilt für Regelungslücken.

ANHANG I - LISTE DER PARTEIEN

Hinweis zur Identifikation der Parteien

Dieser AVV wird nicht gesondert unterzeichnet. Die Identifikation der Parteien erfolgt ausschließlich über den zugrundeliegenden Hauptvertrag (SaaS-Vertrag), in dem dieser AVV durch ausdrückliche Bezugnahme Vertragsbestandteil wird. Mit Abschluss des Hauptvertrags erkennt der Verantwortliche diesen AVV als verbindlich an.

Verantwortlicher

Bezeichnung	Der im Hauptvertrag als Kunde bezeichnete Vertragspartner der iDWELL GmbH
Anschrift	Gemäß Angaben im Hauptvertrag
Ansprechpartner	Gemäß Angaben im Hauptvertrag bzw. gemäß der im Kunden-Account hinterlegten Kontaktdaten
Datenschutzbeauftragter	Sofern vom Verantwortlichen benannt, gemäß Angaben im Hauptvertrag oder im Kunden-Account
Rolle	Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO

Auftragsverarbeiter

Bezeichnung	iDWELL GmbH
Anschrift	Margaretenstraße 70/2/7, 1050 Wien, Österreich
Firmenbuchnummer	FN 484820 h (Handelsgericht Wien)
Telefon	+49 89 997436845
E-Mail (allgemein)	kontakt@idwell.com
Ansprechpartner	Alexander Roth, CEO, alexander.roth@idwell.com
Datenschutz-Kontakt	datenschutz@idwell.com
Rolle	Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO

Keine Unterschrift erforderlich

Dieser AVV wird durch die Einbeziehung im Hauptvertrag wirksam. Eine gesonderte Unterzeichnung, Paraphierung oder sonstige förmliche Annahme ist - weder in Schrift-, noch in Textform - erforderlich. Die jeweils gültige Fassung ist online abrufbar unter https://www.idwell.com/de/dpa. Die zum Zeitpunkt des Abschlusses des Hauptvertrags gültige Fassung ist für die Parteien verbindlich; spätere Aktualisierungen richten sich nach Klausel 11.

ANHANG II - BESCHREIBUNG DER VERARBEITUNG

> **Modularer Aufbau**
> Der konkrete Verarbeitungsumfang richtet sich nach den vom Verantwortlichen im Hauptvertrag gebuchten Modulen. Nicht gebuchte Module begründen keine Verarbeitung im Sinne dieses Anhangs. Die nachfolgenden Abschnitte A bis D sind daher kumulativ anwendbar, je nach dem vom Kunden konkret genutzten Funktionsumfang.

A. Allgemeine Angaben (produktübergreifend)

A.1 Art der Verarbeitung

Erhebung, Erfassung, Organisation, Ordnung, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung, Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschung und Vernichtung personenbezogener Daten im Rahmen des Betriebs und der Bereitstellung der iDWELL-Plattform und der darin enthaltenen Module.

A.2 Gegenstand und Zweck der Verarbeitung

Bereitstellung einer 360°-SaaS-Plattform für die Immobilienverwaltung zugunsten des Verantwortlichen, einschließlich der Kommunikation mit Mietern, Eigentümern und Dienstleistern, des Ticketing- und Schadensmanagements, der Dokumenten- und Rechnungsverwaltung sowie der damit verbundenen Automatisierungs- und Integrationsfunktionen.

A.3 Hosting und Verarbeitungsorte

Die Hauptverarbeitung und Speicherung erfolgt auf Servern innerhalb der Europäischen Union (AWS, Region Frankfurt am Main, Deutschland). Details zu eingesetzten Unterauftragsverarbeitern und deren Verarbeitungsorten ergeben sich aus Anhang IV.

A.4 Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des Hauptvertrags und der darin vereinbarten Nutzung der iDWELL-Plattform. Nach Beendigung des Hauptvertrags werden die Daten gemäß Klausel 10 gelöscht bzw. zurückgegeben, vorbehaltlich gesetzlicher Aufbewahrungspflichten (insbesondere im Modul iDWELL Finance, vgl. Abschnitt C.4).

A.5 Kategorien betroffener Personen (produktübergreifend)

- Mitarbeiter und Nutzer des Verantwortlichen (Hausverwalter, Buchhalter, Administratoren)
- Kunden des Verantwortlichen (Mieter und Eigentümer)
- Lieferanten und Dienstleister (Handwerker, Hausmeister, Serviceunternehmen)
- Beteiligte Dritte (z. B. Familienmitglieder, Bevollmächtigte, Beiratsmitglieder, WEG-Verwalter)
- Außendienstmitarbeiter
- Rechnungsaussteller und deren Ansprechpartner (insbesondere im Modul iDWELL Finance)

A.6 Allgemeine Kategorien personenbezogener Daten (produktübergreifend)

- Namensdaten (Vorname, Nachname, ggf. Titel)
- Kontaktdaten (E-Mail-Adresse, Telefon-/Mobilnummer, Anschrift, Objektzuordnung)
- IT-Nutzungsdaten (Login-Informationen, IP-Adressen, Session-Daten, Logfiles)
- Kommunikationsinhalte (Nachrichten, Tickets, Kommentare, hochgeladene Dokumente)
- Tätigkeits- und Nutzungsdaten (Effektivitätsmessungen wie Antwortgeschwindigkeit, Anzahl erstellter oder bearbeiteter Servicemeldungen, Nutzerverhalten)

B. Modul iDWELL CRM, Kunden-App, Services und Digitales Schwarzes Brett

B.1 Gegenstand und Zweck

Übertragung der Mieter- und Eigentümerdaten (in Kopie) zur Bereitstellung dieser Daten auf der Plattform idwell.com. Die Daten werden benötigt, um sie den Mitarbeitern des Verantwortlichen für eine ordnungsgemäße Bearbeitung auf der Kommunikations- und Ticketing-Plattform (CRM) zur Verfügung zu stellen. Darüber hinaus werden die Daten verarbeitet, um individualisierte Profile auf der iDWELL Kunden-App für Mieter und Eigentümer zu erstellen,

Dienstleistern die Bearbeitung von Tickets im Rahmen der Service-Plattform zu ermöglichen sowie die Funktion „Digitales Schwarzes Brett" bereitzustellen.

B.2 Spezifische Kategorien personenbezogener Daten

- Identifikations- und Stammdaten (Vorname, Nachname, Geburtsdatum - soweit vom Verantwortlichen eingebracht)
- Kontaktdaten (E-Mail, Telefon, Anschrift, Objekt- und Einheitszuordnung)
- Vertrags- und Verwaltungsdaten (Mieter-/Eigentümerstatus, Einheitennummer, Miteigentumsanteile, WEG-Zugehörigkeit - soweit eingebracht)
- Kommunikationsinhalte (Ticketinhalte, Nachrichten, Schadensmeldungen, Fotos, Dateianhänge)
- Nutzungsdaten der App (Login-Zeitpunkte, genutzte Funktionen, Push-Notification-Präferenzen)
- Dienstleisterdaten (Name, Kontakt, Tätigkeitsbereich, Zugangszeiten)
- Daten im Digitalen Schwarzen Brett (Aushänge, Informationen, hochgeladene Dokumente)

B.3 Kategorien betroffener Personen (modulspezifisch)

- Mieter, Eigentümer und deren Haushaltsangehörige (soweit in Stammdaten erfasst)
- Mitarbeiter des Verantwortlichen (Sachbearbeiter, Hausverwalter)
- Dienstleister und deren Mitarbeiter
- Beiratsmitglieder, Verwaltungsbeiräte, WEG-Organe

B.4 Dauer

Für die Dauer des Hauptvertragsverhältnisses und der Nutzung der Services durch den Verantwortlichen. Nach Beendigung gemäß Klausel 10.

C. Modul iDWELL Finance (KI-gestützte Rechnungsverarbeitung)

> **Hinweis - iDWELL Finance**
> Das Modul iDWELL Finance digitalisiert den gesamten Zyklus des Rechnungsmanagements. Vom Rechnungseingang über den Genehmigungs-Workflow bis hin zur Integration mit Buchhaltungssystemen und Online-Banking. Es umfasst KI-basierte Belegerkennung, Duplikats-Check, digitale Rechnungsprüfung, Kontierungsvorschläge, ein revisionssicheres Archiv (GoBD-konform) sowie Schnittstellen zu ERP-Systemen. Für dieses Modul gelten ergänzend zu den allgemeinen Regelungen die nachfolgenden Bestimmungen.

C.1 Gegenstand und Zweck

Automatisierte Erfassung, Extraktion, Prüfung, Freigabe, Kontierung, revisionssichere Archivierung sowie Übermittlung von Eingangsrechnungen und damit verbundenen Buchhaltungsbelegen.

Die Verarbeitung umfasst die KI-basierte Erkennung von Rechnungsdetails (einschließlich der Objektadresse) ohne vorheriges Training, die Unterstützung ein- oder mehrstufiger Freigabeprozesse, die Erzeugung von Kontierungsvorschlägen, die Erkennung von Duplikaten sowie die Übertragung freigegebener Rechnungen an Buchhaltungs- und Online-Banking-Systeme des Verantwortlichen.

C.2 Spezifische Kategorien personenbezogener Daten

- Identifikations- und Kontaktdaten von Rechnungsausstellern (Firmen, Einzelunternehmer, Freiberufler) und deren Ansprechpartnern (Name, Anschrift, E-Mail, Telefon)
- Steuerliche Identifikationsmerkmale (UID-Nummer / USt-IdNr., Steuernummer, Firmenbuchnummer/Handelsregisternummer)
- Bank- und Zahlungsverbindungsdaten (IBAN, BIC, Kontoinhaber, Verwendungszweck, Zahlungsreferenz - sowohl von Lieferanten als auch gegebenenfalls von natürlichen Personen als Rechnungsausstellern)
- Rechnungsinhaltsdaten (Rechnungsnummer, Rechnungsdatum, Leistungszeitraum, Einzelpositionen, Mengen, Einzel- und Gesamtbeträge, Steuerbeträge und -sätze, Zahlungsbedingungen, Skonto)
- Objekt- und Liegenschaftszuordnungen (erkannte Objektadresse, Einheitenbezug, Kostenstelle)
- Workflow- und Freigabedaten (Identität des freigebenden Mitarbeiters, Freigabezeitpunkt, Kommentare, elektronische Freigabe-/Prüfvermerke, ggf. elektronische Signatur)

- Kontierungsdaten (Sachkonten, Debitoren-/Kreditorenkonten, Kostenstellen, Buchungstexte)
- Kommunikations- und Abstimmungsdaten zum Beleg (Nachrichten zwischen Mitarbeitern und Lieferanten direkt am Beleg, Rückfragen, Klärungen)
- Metadaten und Protokolldaten (Uploadzeitpunkt, Bearbeitungsverlauf, Änderungshistorie, Audit-Trail zur Erfüllung der GoBD-Anforderungen)
- Inhalte beigefügter Dokumente (z. B. Lieferscheine, Angebote, Gutschriften, Mahnungen, Leistungsnachweise) - soweit personenbezogene Daten enthalten

C.3 Kategorien betroffener Personen (modulspezifisch)

- Rechnungsaussteller, soweit natürliche Personen (z. B. Einzelunternehmer, Freiberufler, Selbständige Handwerker)
- Ansprechpartner von Lieferantenunternehmen (Kontaktpersonen in Rechnungen)
- Mitarbeiter des Verantwortlichen mit Freigabe-, Prüf- oder Kontierungsrechten
- Kontoinhaber von Bankverbindungen, die in Rechnungen angegeben sind
- Debitoren und Kreditoren des Verantwortlichen, soweit natürliche Personen

C.4 Dauer der Verarbeitung und gesetzliche Aufbewahrungsfristen

Die Verarbeitung erfolgt für die Dauer des Hauptvertragsverhältnisses. Abweichend von der allgemeinen Löschungsregelung gemäß Klausel 10 bleiben Rechnungen und damit verbundene Buchhaltungsunterlagen zur Erfüllung handels- und steuerrechtlicher Aufbewahrungspflichten erhalten:

- **Österreich:** 7 Jahre gemäß § 132 Abs. 1 BAO sowie § 212 UGB (teilweise längere Fristen bei Grundstücken)
- **Deutschland:** 10 Jahre gemäß § 147 AO, § 257 HGB und den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)

Während dieser gesetzlichen Aufbewahrungsfristen werden die betroffenen Daten in einem revisionssicheren Archiv gespeichert, zugriffsbeschränkt und ausschließlich zum Zweck der Erfüllung der gesetzlichen Aufbewahrungspflicht verarbeitet. Nach Ablauf der gesetzlichen Fristen erfolgt eine Löschung gemäß Klausel 10.

C.5 KI-gestützte Verarbeitung und Sub-Auftragsverarbeitung durch Blumatix Intelligence GmbH

Im Rahmen des Moduls iDWELL Finance setzt der Auftragsverarbeiter die Blumatix Intelligence GmbH („bluDELTA Service“) als Sub-Auftragsverarbeiterin zur automatisierten Erkennung und Extraktion von Rechnungsdaten ein. Übermittelt werden ausschließlich die vom Verantwortlichen aktiv zur Verarbeitung freigegebenen Eingangsdokumente (insbesondere Rechnungen, Lieferscheine und vergleichbare Geschäftsdokumente).

Die Verarbeitung dauert in der Regel nur wenige Sekunden bis Minuten pro Dokument. Eine dauerhafte Speicherung der Dokumente bei Blumatix erfolgt nicht, soweit dies nicht zur Vertragserfüllung technisch erforderlich ist.

Die Verarbeitung erfolgt ausschließlich innerhalb der Europäischen Union. Eine Übermittlung in Drittländer findet im Rahmen dieses Sub-Auftragsverarbeitungsverhältnisses nicht statt.

Bei KI-gestützten Verarbeitungen kann technologiebedingt eine fortlaufende Verbesserung der eingesetzten Modelle stattfinden. Im produktiven Betrieb werden die von iDWELL übermittelten Dokumente ausschließlich zur Erbringung der vereinbarten Serviceleistung verarbeitet.

Eine dauerhafte Speicherung erfolgt - wie im AVV beschrieben - nicht (Dokumente im Produktivbetrieb werden grundsätzlich nicht persistent gespeichert, sofern dies nicht zur Vertragserfüllung erforderlich ist.).

Eine Verwendung von Daten für Training, Benchmarking oder Weiterentwicklung erfolgt nur dann, wenn Blumatix diese von iDWELL aktiv und explizit zu diesem Zweck zur Verfügung gestellt werden. Z.B. via Support.

Der Verantwortliche kann jederzeit über die in diesem AVV vorgesehenen Auskunfts- und Kontrollrechte nähere Informationen zur konkreten Ausgestaltung der Verarbeitung durch Blumatix anfordern.

Wesentliche Änderungen der Verarbeitung, insbesondere im Hinblick auf den Umgang mit KI-Modelltraining, werden dem Verantwortlichen gemäß den Regelungen dieses AVV zu Sub-Auftragsverarbeitern mitgeteilt.

C.6 Integrationen mit Buchhaltungs- und Banking-Systemen

Sofern der Verantwortliche Schnittstellen zu Buchhaltungssystemen (ERP/FIBU) oder Online-Banking-Systemen aktiviert, übermittelt das Modul iDWELL Finance freigegebene Rechnungs- und Zahlungsdaten an die vom Verantwortlichen spezifizierten Zielsysteme.

Diese Systeme liegen außerhalb des Verantwortungsbereichs des Auftragsverarbeiters; die Einrichtung, Konfiguration und die datenschutzrechtliche Bewertung der Zielsysteme obliegt dem Verantwortlichen. Der Auftragsverarbeiter setzt keine eigenen Weisungen zur Datenübermittlung an diese Zielsysteme um, die über die durch den Verantwortlichen aktivierte Konfiguration hinausgehen.

C.7 Internes Kontrollsystem (IKS) und Zugriffsbeschränkungen

Das Modul iDWELL Finance verfügt über ein integriertes internes Kontrollsystem (IKS) sowie eine feingranulare Rechteverwaltung. Der Verantwortliche ist für die Konfiguration der Zugriffsrechte seiner Mitarbeiter (Vier-Augen-Prinzip, Freigabelimits, Rollentrennung) selbst verantwortlich und stellt sicher, dass der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) eingehalten wird.

ANHANG III - TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM)

Gemäß Art. 32 DSGVO hat der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Dazu zählen insbesondere die nachfolgenden Maßnahmen, wobei insbesondere die mit der Datenverarbeitung zusammenhängenden Risiken (etwa unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugter Zugang) zu berücksichtigen sind. Die Überschriften dienen lediglich der besseren Einordnung und haben keinen Einfluss auf das Ausmaß der jeweiligen Maßnahme.

Anlage 1 - Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Vertraulichkeit / Zugangskontrolle Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet? Vertraulichkeit bedeutet, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.	✓ Elektronisches Zutrittskontrollsystem ✓ Alarmanlage ✓ Videoüberwachung ✓ Spezielle Schutzvorkehrungen für den Serverraum (bei Unterauftragsverarbeitern) ✓ Individueller Login und Kennwortverfahren ✓ Zusätzlicher Login für bestimmte Anwendungen / Multi-Faktor-Authentifizierung (MFA) ✓ Automatische Sperrung der Clients (Zeitablauf) ✓ Rollen- und rechtebasierte Berechtigungsverwaltung ✓ Dokumentation von Berechtigungen ✓ Verschlüsselung von Systemen (at rest) ✓ Verschlüsselung der Kommunikation (TLS ≥ 1.2) ✓ Verschlüsselung von Datenträgern ✓ VPN (Virtual Private Network) ✓ Gesichertes WLAN (WPA2/WPA3) ✓ SSL-/TLS-Verschlüsselung bei Web-Access ✓ Passwortrichtlinie (Mindestlänge 8 Zeichen, Komplexitätsregeln) ✓ Antivirensoftware ✓ Firewall ✓ Automatische Bildschirmsperre
Integrität Wie wird die Integrität der Daten dauerhaft gewährleistet? Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.	✓ Verwendung von Zugriffsrechten ✓ Systemseitige Protokollierungen (Audit-Logs) ✓ Funktionelle Verantwortlichkeiten / Rollentrennung ✓ Revisionssicheres Archiv für iDWELL Finance (unveränderliche Speicherung, lückenlose Änderungshistorie, GoBD-konform) ✓ Prüfsummen / Hash-Verfahren zur Sicherstellung der Datenintegrität bei Rechnungs- und Belegdaten
Verfügbarkeit Wie wird die Verfügbarkeit der Daten dauerhaft gewährleistet?	✓ Back-Up-Verfahren (täglich, inkl. Offsite-Backup) ✓ Spiegeln von Festplatten (RAID) ✓ Unterbrechungsfreie Stromversorgung (USV) ✓ Virenschutz / Firewall ✓ Notfallplan / Business Continuity Plan ✓ Klimaanlagen in Rechenzentren (bei AWS) ✓ Brand- und Löschwasserschutz ✓ Alarmanlage ✓ Geeignete Archivierungsräumlichkeiten
Belastbarkeit Wie wird die Belastbarkeit der Systeme dauerhaft gewährleistet?	✓ Penetrationstests (regelmäßig durch externe Dienstleister) ✓ Lasttests ✓ Skalierbare Cloud-Infrastruktur (AWS) ✓ Monitoring und Alerting
Wiederherstellbarkeit der Verfügbarkeit und des Zugangs Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?	✓ Back-Up-Verfahren mit definierten Recovery Time / Recovery Point Objectives (RTO/RPO) ✓ Unterbrechungsfreie Stromversorgung (USV) ✓ Notfallplan / Desaster-Recovery-Plan ✓ Vertretungsregelungen ✓ Regelmäßige Restore-Tests

Pseudonymisierung Wie wird die Pseudonymisierung der Daten gewährleistet?	✓ Personenbezogene Daten werden - wo möglich - durch Zufallscodes/IDs ersetzt ✓ Data Masking in Test- und Entwicklungssystemen ✓ Für produktive Nutzerdaten ist eine vollständige Pseudonymisierung aufgrund der Zweckbestimmung (Kommunikation, Rechnungsbezug) nicht durchgehend möglich
Verschlüsselung Wie wird die Verschlüsselung gewährleistet?	✓ Verschlüsselung der Kommunikation (TLS ≥ 1.2) ✓ Verschlüsselung von Speichermedien (at rest) ✓ Data Hashing (z. B. für Passwörter mit Salt) ✓ Amazon S3 wendet serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) als Basisverschlüsselung für jeden Bucket in Amazon S3 an ✓ Verwendung kryptographischer Tools nach Stand der Technik
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?	✓ Festgelegte Prüfroutine ✓ Prüfberichte werden evaluiert ✓ Implementierung von Verbesserungsvorschlägen ✓ Datenschutzmanagementsystem (DSMS) ✓ Jährliche Überprüfung der TOM
Verhinderung unrechtmäßigen Zugangs zu personenbezogenen Daten Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?	✓ Individueller Login und Kennwortverfahren ✓ Zusätzlicher Login für bestimmte Anwendungen / MFA ✓ Automatische Sperrung der Clients (Zeitablauf) ✓ Rollen- und rechtebasierte Berechtigungsverwaltung ✓ Dokumentation von Berechtigungen ✓ Verschlüsselung von Systemen ✓ Erweiterte Logging- und Monitoring-Mechanismen für iDWELL Finance (Audit-Trail für Zugriffe auf Rechnungs- und Zahlungsdaten)
Verarbeitung personenbezogener Daten nur nach Anweisung Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?	✓ Mitarbeiter sind zu Verhaltensregeln verpflichtet ✓ Verpflichtung der Mitarbeiter auf das Datengeheimnis (Art. 28 Abs. 3 lit. b DSGVO, § 6 DSG, § 53 BDSG) ✓ Schulungen aller zugriffsberechtigten Mitarbeiter (mindestens jährlich) ✓ Bestimmung von Ansprechpartnern für den konkreten Auftrag ✓ Interner Datenschutz-Verantwortlicher benannt (datenschutz@idwell.com)
Allgemeine Anforderungen	✓ Regelmäßige Durchführung von Updates und Patches ✓ Implementierung unternehmensinterner Datenschutz-Richtlinien ✓ Kontrollierte Fernwartungen (nur mit Zustimmung und Protokollierung) ✓ Zertifizierungen: ISO-Zertifizierung des AWS Cloud Services (u. a. ISO 27001, ISO 27017, ISO 27018) ✓ Regelmäßige Penetrationstests der Applikation ✓ Dokumentierte Sub-Auftragsverarbeiter-Prüfung vor Beauftragung ✓ Incident-Response-Prozess mit definierten Meldewegen

ANHANG IV - LISTE DER (UNTER-)AUFTRAGSVERARBEITER

Die nachstehende Liste enthält die zum Zeitpunkt der letzten Aktualisierung dieses AVV eingesetzten (Unter-)Auftragsverarbeiter.

Anbieter	Anschrift	Kontakt	Rolle / Zweck
Amazon Web Services EMEA SARL (AWS)	AWS EU Frankfurt Region (Region Frankfurt am Main, Deutschland)	https://aws.amazon.com/de/contact-us/compliance-support/	Hosting und Infrastruktur (Cloud-Speicherung und -verarbeitung); gilt für alle iDWELL-Produkte
Blumatix Intelligence GmbH	Schwarzstraße 48, 5020 Salzburg, Österreich	office@blumatix.com | www.blumatix.com	KI-gestützte Rechnungs- und Belegerkennung (bluDELTA Service); ausschließlich im Modul iDWELL Finance

Hinweise zu Unterauftragsverarbeitern

1. Infrastruktur- und Support-Dienstleister, die ausschließlich Dienstleistungen gegenüber dem Auftragsverarbeiter selbst erbringen und dabei nur inzidentell auf personenbezogene Daten zugreifen können (z. B. Rechenzentrums-Dienstleistungen, Telekommunikationsanbieter, Postdienstleister, Wirtschaftsprüfer, Steuerberater, Rechtsanwälte mit Berufsgeheimnisverpflichtung), gelten nicht als Unterauftragsverarbeiter im Sinne des Art. 28 DSGVO.

2. Soweit der Verantwortliche selbst Integrationen oder Schnittstellen zu Drittsystemen aktiviert (vgl. Anhang II Abschnitt D), liegt die Auswahl, Beauftragung und datenschutzrechtliche Bewertung dieser Drittsysteme ausschließlich in seinem Verantwortungsbereich.

Hinweis zur KI-gestützten Verarbeitung im Modul iDWELL Finance

Betrifft ausschließlich das Modul iDWELL Finance

Im Rahmen des Moduls iDWELL Finance setzt die iDWELL GmbH die Blumatix Intelligence GmbH („bluDELTA Service“) als Sub-Auftragsverarbeiterin zur automatisierten Erkennung und Extraktion von Rechnungsdaten ein. Übermittelt werden ausschließlich die vom Verantwortlichen aktiv zur Verarbeitung freigegebenen Eingangsdokumente (insbesondere Rechnungen, Lieferscheine und vergleichbare Geschäftsdokumente). Die Verarbeitung dauert in der Regel nur wenige Sekunden bis Minuten pro Dokument. Eine dauerhafte Speicherung der Dokumente bei Blumatix erfolgt nicht, soweit dies nicht zur Vertragserfüllung technisch erforderlich ist.

Die Verarbeitung erfolgt ausschließlich innerhalb der Europäischen Union. Eine Übermittlung in Drittländer findet im Rahmen dieses Sub-Auftragsverarbeitungsverhältnisses nicht statt.

Bei KI-gestützten Verarbeitungen kann technologiebedingt eine fortlaufende Verbesserung der eingesetzten Modelle stattfinden.Wesentliche Änderungen der Verarbeitung, insbesondere im Hinblick auf den Umgang mit KI-Modelltraining, werden dem Verantwortlichen gemäß den Regelungen dieses AVV zu Sub-Auftragsverarbeitern mitgeteilt.