AUFTRAGSVERARBEITUNGSVERTRAG (AVV) gemäß Art. 28 Abs. 3 DSGVO

zwischen dem Verantwortlichen und dem Auftragsverarbeiter

Stand: Oktober 2025 | **Version:** 2.0

PRÄAMBEL

Dieser Auftragsverarbeitungsvertrag (AVV) regelt die Verarbeitung personenbezogener Daten im Rahmen der Buchhaltungsdienstleistungen gemäß dem zwischen den Parteien geschlossenen Rahmenvertrag für Buchhaltungsdienstleistungen (nachfolgend „**Hauptvertrag**").

Mit diesem AVV soll die Einhaltung von **Art. 28 Abs. 3 und 4 der Datenschutz-Grundverordnung (DSGVO)** sichergestellt werden.

ABSCHNITT I - ZWECK UND ANWENDUNGSBEREICH

Klausel 1: Zweck und Anwendungsbereich

a) Mit diesem Auftragsverarbeitungsvertrag (im Folgenden „Klauseln") soll die Einhaltung von Art. 28 Abs. 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (Datenschutz-Grundverordnung, DSGVO) im Rahmen der Buchhaltungsdienstleistungen durch den Auftragsverarbeiter gemäß dem Hauptvertrag sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Art. 28 Abs. 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 der Klauseln.

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. Da die Datenverarbeitung ausschließlich innerhalb der Europäischen Union erfolgt, sind keine zusätzlichen Garantien nach Kapitel V DSGVO erforderlich.

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 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen.

c) Diese Klauseln dürfen 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 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 Unterzeichnung 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 des Auftragsverarbeiters

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.

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 zusätzliche Garantien an.

Hinweis: Bei Lohnbuchhaltung können Gesundheitsdaten (Krankmeldungen, Schwerbehinderteneigenschaft) anfallen. In diesen Fällen gelten erhöhte Anforderungen.

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 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 **Anhang IV** aufgeführt sind.

Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens **zwei Wochen im Voraus** ausdrücklich in **schriftlicher Form** (E-Mail ausreichend) 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.

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 im Einklang stehen.

b) Für die Verarbeitung im Rahmen dieses AVV gilt: Alle Daten werden ausschließlich auf Servern in der Europäischen Union verarbeitet und gespeichert. Eine Übermittlung in Drittländer findet nicht statt.

Sollte zukünftig eine Übermittlung in Drittländer erforderlich werden (z.B. durch Einbindung von Cloud-Diensten außerhalb der EU), wird der Auftragsverarbeiter den Verantwortlichen vorab informieren und die Einhaltung von Kapitel V DSGVO durch geeignete Garantien (z.B. EU-Standardvertragsklauseln) sicherstellen.

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.

Dies umfasst insbesondere:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

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 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 Art. 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:

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 Art. 33 Abs. 3 DSGVO 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 Art. 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.

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 Art. 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 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 nicht erfüllt;

3. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der DSGVO 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.

Gemäß § 10 des Hauptvertrags stellt Bilancor dem Mandanten nach Vertragsende alle Daten für 30 Tage zum Download bereit, danach erfolgt die Löschung.

ANHANG I - LISTE DER PARTEIEN

Verantwortlicher:

Name: [Name des Mandanten]
Anschrift: [Adresse des Mandanten]
Kontaktperson: [Name, E-Mail, Telefon]

Rolle: Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO

Auftragsverarbeiter:

Name: Bilancor GmbH
Anschrift: Richard-Ermisch-Str. 7, 10247 Berlin
Handelsregister: Amtsgericht Charlottenburg, HRB 279439 B
Geschäftsführung: Carsten Lebtig

Kontaktpersonen:
Richard Jülly: rj@bilancor.de
Nicholas Kummer: nk@bilancor.de

Rolle: Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO

ANHANG II - BESCHREIBUNG DER VERARBEITUNG

1. Gegenstand und Dauer der Verarbeitung

Gegenstand:
Verarbeitung personenbezogener Daten im Rahmen der Erbringung von Buchhaltungsdienstleistungen gemäß dem zwischen den Parteien geschlossenen Rahmenvertrag für Buchhaltungsdienstleistungen.

Dauer:
Die Dauer der Datenverarbeitung entspricht der Laufzeit des Hauptvertrags zuzüglich der Aufbewahrungsfrist von 30 Tagen nach Vertragsende (gemäß § 10.2 des Hauptvertrags).

---

2. Art und Zweck der Verarbeitung

Art der Verarbeitung:

- Erheben
- Erfassen
- Organisation
- Ordnen
- Speicherung
- Anpassung oder Veränderung
- Auslesen
- Abfragen
- Verwendung
- Offenlegung durch Übermittlung (nur an Steuerberater-Partner des Verantwortlichen, soweit vom Verantwortlichen beauftragt)
- Abgleich oder Verknüpfung
- Einschränkung
- Löschen oder Vernichten

Zweck der Verarbeitung:

Die Datenverarbeitung dient ausschließlich der Erfüllung der vertraglich vereinbarten Buchhaltungsdienstleistungen, insbesondere:

- Laufende Finanzbuchhaltung (Erfassung und Verbuchung von Geschäftsvorfällen)
- Erstellung von betriebswirtschaftlichen Auswertungen (BWA)
- Vorbereitung von Umsatzsteuer-Voranmeldungen
- Vorbereitung von Jahresabschlüssen (EÜR)
- Lohnbuchhaltung (falls vereinbart)
- Digitale Belegverwaltung
- Bereitstellung von Auswertungen und Berichten über die Bilancor-Plattform

---

3. Kategorien betroffener Personen

a) Bei Finanzbuchhaltung:

- Kunden des Verantwortlichen (Debitoren)
- Lieferanten des Verantwortlichen (Kreditoren)
- Geschäftspartner
- Dienstleister

b) Bei Lohnbuchhaltung (falls beauftragt):

- Arbeitnehmer des Verantwortlichen
- Bewerber
- Freie Mitarbeiter / Freelancer
- Geringfügig Beschäftigte (Minijobber)

c) Sonstige:

- Vertreter juristischer Personen (Geschäftsführer, Vorstände)

- Ansprechpartner bei Geschäftspartnern

---

4. Kategorien personenbezogener Daten

a) Stammdaten:

- Name, Vorname
- Firmenbezeichnung
- Anschrift (Straße, PLZ, Ort, Land)
- Kontaktdaten (Telefon, E-Mail, Fax)
- Bankverbindung (IBAN, BIC)
- Steuernummer, Umsatzsteuer-Identifikationsnummer (USt-ID)
- Handelsregisternummer

b) Vertragsdaten:

- Kundennummer, Lieferantennummer, Kreditorennummer, Debitorennummer
- Rechnungsinformationen (Rechnungsnummer, Datum, Betrag, Zahlungsbedingungen)
- Zahlungshistorie
- Vertragslaufzeiten

c) Finanzdaten:

- Kontobewegungen (Datum, Betrag, Verwendungszweck, Gegenpartei)
- Offene Posten
- Mahnwesen-Daten

d) Bei Lohnbuchhaltung zusätzlich (falls beauftragt):

- Personalnummer
- Geburtsdatum, Geburtsort
- Staatsangehörigkeit
- Familienstand
- Steuerklasse, Kinderfreibeträge
- Sozialversicherungsnummer
- Steuer-Identifikationsnummer
- Krankenversicherung (Name der Krankenkasse)
- Eintrittsdatum, Austrittsdatum
- Gehaltsdaten (Brutto, Netto, Abzüge)
- Arbeitszeitdaten (Stunden, Urlaub, Krankheit)
- Bankverbindung für Gehaltszahlung

e) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO):

Im Regelfall werden keine besonderen Kategorien personenbezogener Daten verarbeitet.

Ausnahme bei Lohnbuchhaltung (falls relevant):

- Gesundheitsdaten (nur soweit für Lohnabrechnung erforderlich, z.B. Krankmeldungen, Schwerbehinderteneigenschaft für steuerliche Freibeträge)

In diesen Fällen werden erhöhte technische und organisatorische Maßnahmen gemäß Anhang III angewendet.

---

5. Ort der Verarbeitung

Die Datenverarbeitung erfolgt ausschließlich in der Europäischen Union (EU).

Daten sind in Europa gehostet und verschlüsselt und die Verarbeitung personenbezogener Daten ist komplett DSGVO-konform. Die Anmeldung sowie sensible Vorgänge werden durch eine Zwei-Faktor-Authentifizierung geschützt.

Eine Übermittlung in Drittländer außerhalb der EU/EWR findet nicht statt.

ANHANG III - TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMs)

Gemäß Art. 32 DSGVO trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

---

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Ziel: Unbefugten Personen wird der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt.

Maßnahme	**Beschreibung**	**Umsetzung Bilancor**
Physische Zugangssicherung	Schutz der Räumlichkeiten vor unbefugtem Zutritt	Büroräume mit Zugangskontrolle (Schlüssel/Chipkarte)
Mitarbeiterschulung	Sensibilisierung für Datenschutz	Verpflichtung auf Vertraulichkeit (§ 203 StGB), Regelmäßige Datenschutz-Schulungen

Clean Desk Policy	Keine Unterlagen mit personenbezogenen Daten unbeaufsichtigt	Verschließbare Schränke, Bildschirmsperre bei Abwesenheit

1.2 Zugangskontrolle

Ziel: Verhinderung, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Benutzerauthentifizierung	Zugriff nur mit persönlichen Zugangsdaten	Individuelle Benutzerkonten, Starke Passwortrichtlinien (min. 12 Zeichen, Komplexität), Zwei-Faktor-Authentifizierung (2FA) für Plattformzugang
Zugriffsrechteverwaltung	Rechtevergabe nach Need-to-know-Prinzip	Rollenbasiertes Zugriffskonzept, Regelmäßige Überprüfung der Berechtigungen, Entzug bei Ausscheiden von Mitarbeitern
Protokollierung	Nachvollziehbarkeit von Zugriffen	Logging aller System-Zugriffe, Aufbewahrung der Logs für 90 Tage
Firewall & VPN	Schutz vor externen Angriffen	Enterprise-Firewall, VPN-Pflicht bei Remote-ZugriffVerschlüsselte Verbindungen (TLS 1.3)

1.3 Zugriffskontrolle

Ziel: Gewährleistung, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Mandantentrennung	Strikte Trennung der Daten verschiedener Mandanten	Logische Mandantentrennung in der Datenbank, Technische Zugriffsbeschränkung (Mitarbeiter sehen nur zugewiesene Mandanten)
Berechtigungskonzept	Differenzierte Rechtevergabe	Zugriff nur auf notwendige Daten, Vier-Augen-Prinzip bei sensiblen Vorgängen (z.B. Lohndaten)

Verschlüsselung	Schutz bei unbefugtem Zugriff	Datenbankverschlüsselung (AES-256), Verschlüsselte Datenspeicherung auf Servern

1.4 Trennungskontrolle

Ziel: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Zweckbindung	Daten werden nur für den vereinbarten Zweck verarbeitet	Datenverarbeitung ausschließlich für Buchhaltung, Keine Nutzung für Marketing oder andere Zwecke
Systemtrennung	Unterschiedliche Systeme für unterschiedliche Zwecke	Produktivsystem getrennt von Test-/Entwicklungssystem, Keine Produktivdaten in Testumgebungen

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Ziel: Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Pseudonymisierung bei Entwicklung/Tests	Verwendung anonymisierter Testdaten	Keine echten Mandantendaten in Entwicklung, Generierung synthetischer Testdaten
Interne Kennungen	Verwendung interner IDs statt Namen	Technische IDs für Datenbankabfragen, Personenbezug nur bei Bedarf hergestellt

---

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Ziel: Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**

Transportverschlüsselung	Verschlüsselte Datenübertragung	TLS 1.3 für alle Verbindungen (Plattform, E-Mail) - HTTPS für Web-Zugriff - Verschlüsselte SFTP für Datei-Uploads
E-Mail-Verschlüsselung	Schutz sensibler Daten per E-Mail	Hinweis an Mandanten: Keine sensiblen Daten per unverschlüsselter E-Mail - Nutzung der Plattform (verschlüsselt) bevorzugt
Protokollierung Datenexporte	Nachvollziehbarkeit von Datenübermittlungen	Logging aller Datenexporte (z.B. Download durch Mandant, Übergabe an Steuerberater) - Dokumentation des Empfängers

2.2 Eingabekontrolle

Ziel: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Protokollierung Dateneingabe	Nachvollziehbarkeit aller Änderungen	Logging von Erstanlage, Änderung, Löschung - Speicherung: Wer, Was, Wann - Versionierung von Buchungen
Audit-Trail	Änderungshistorie	Unveränderliche Protokolle (Append-only) - Regelmäßige Kontrolle durch Qualitätssicherung

---

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

Ziel: Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**

Backup-Strategie	Regelmäßige Datensicherungen	Tägliche automatische Backups, Aufbewahrung: 30 Tage, Speicherung geografisch getrennt (anderes Rechenzentrum)
Backup-Tests	Überprüfung der Wiederherstellbarkeit	Vierteljährliche Test-Wiederherstellungen, Dokumentation der Tests
Hochverfügbarkeit	Redundante Systeme	Redundante Server-Infrastruktur Load Balancing, Ziel: 97% Verfügbarkeit (gemäß Hauptvertrag § 4.3)
Unterbrechungsfreie Stromversorgung (USV)	Schutz vor Stromausfall	USV im Rechenzentrum, Notstromaggregate

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

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

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Disaster Recovery Plan	Notfallplan bei Systemausfall	Dokumentiertes Wiederherstellungsverfahren, Recovery Time Objective (RTO): 24 Stunden, Recovery Point Objective (RPO): 24 Stunden
Incident Response Team	Schnelle Reaktion bei Vorfällen	Automatisches Monitoring kritischer Systeme (24/7 automatisch), Alarmmeldungen per E-Mail/SMS an On-Call-Team, Eskalationsprozess: Reaktion innerhalb 2 Stunden (während Servicezeiten), Außerhalb Servicezeiten: Reaktion am nächsten Werktag

---

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**

Datenschutz-Management	Kontinuierliche Verbesserung	Jährliches Datenschutz-Audit, Dokumentation aller Verarbeitungstätigkeiten (Verzeichnis nach Art. 30 DSGVO)
Mitarbeiter-Schulungen	Regelmäßige Sensibilisierung	Jährliche Pflichtschulung Datenschutz, Ad-hoc-Schulungen bei Prozessänderungen
Penetrationstests	Überprüfung der IT-Sicherheit	Jährlicher externer Penetrationstest, Behebung identifizierter Schwachstellen
Software-Updates	Aktuelle Sicherheitsstandards	Regelmäßige Security-Patches, Monatliche Updates, Kritische Patches innerhalb 48h

---

5. Auftragskontrolle

Ziel: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Weisungsbindung	Verarbeitung nur nach Weisung des Verantwortlichen	Verarbeitung ausschließlich gemäß Hauptvertrag und AVV, Keine Eigennutzung der Daten, Bei Unklarheiten: Rückfrage beim Verantwortlichen
Unterauftragsverarbeiter-Management	Sorgfältige Auswahl und Kontrolle	Schriftliche Verträge mit allen Unterauftragsverarbeitern, Prüfung der DSGVO-Konformität, Siehe Anhang IV für Liste

---

6. Vorfallsmanagement (Data Breach)

Ziel: Schnelle Erkennung und Reaktion bei Datenschutzverletzungen.

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Incident Response Plan	Dokumentiertes Verfahren bei Data Breach	Sofortige Meldung an Verantwortlichen (unverzüglich,

		max. 24h), Interne Eskalation, Dokumentation des Vorfalls
Meldewege	Klare Kommunikation	Kontakt für Data Breach: security@bilancor.de, Parallele Information an persönlichen Ansprechpartner

---

7. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Privacy by Design	Datenschutz von Beginn an	Datensparsamkeit: Nur notwendige Daten erfassen - Voreinstellung: Minimale Datenverarbeitung
Privacy by Default	Datenschutzfreundliche Grundeinstellungen	Automatische Löschung nach Vertragsende (30 Tage) - Mandant muss aktiv zustimmen für optionale Features

---

8. Besondere Maßnahmen bei sensiblen Daten (Art. 9 DSGVO)

Nur relevant bei Lohnbuchhaltung mit Gesundheitsdaten:

Maßnahme	**Beschreibung**	**Umsetzung bei Bilancor**
Erweiterte Zugriffsbeschränkungen	Nur autorisierte Mitarbeiter	Vier-Augen-Prinzip bei Gesundheitsdaten, Gesonderte Schulung der Mitarbeiter
Erweiterte Verschlüsselung	Höheres Schutzniveau	Separate Verschlüsselung sensibler Datenfelder, Besondere Protokollierung

---

9. Nachweis der Wirksamkeit

Die Wirksamkeit dieser Maßnahmen wird nachgewiesen durch:

- Dokumentation der TOMs (dieses Dokument)
- Protokollierung (Logs, Audit-Trails)
- Jährliche interne Audits

- Externe Audits/Penetrationstests
- Zertifizierungen (falls vorhanden)

Die TOMs werden bei Bedarf angepasst, um dem Stand der Technik zu entsprechen. Der Verantwortliche wird über wesentliche Änderungen informiert.

ANHANG IV - LISTE DER UNTERAUFTRAGSVERARBEITER

Der Auftragsverarbeiter (Bilancor GmbH) ist gemäß Klausel 7.7 berechtigt, Unterauftragsverarbeiter einzusetzen. Folgende Unterauftragsverarbeiter sind aktuell beauftragt:

---

1. Hosting / Server-Infrastruktur

Unterauftragsverarbeiter	Leistung	Standort	Zweck
[(Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland),] (PENNYLANE SAS RCS : 880 265 921 Paris Siège social : 2-4 rue Jules Lefebvre, 75009 Paris, France]	Server-Hosting, Cloud-Infrastruktur	Deutschland (EU)	Bereitstellung der technischen Infrastruktur für die Bilancor-Plattform

Datenkategorien: Alle im Anhang II genannten personenbezogenen Daten
Vertrag: AVV gemäß Art. 28 DSGVO geschlossen

---

2. KI-Dienstleister / OCR-Technologie

Unterauftragsverarbeiter	Leistung	Standort	Zweck
GFR Software GmbH, Nehringstraße 1, 14059 Berlin	KI-gestützte Belegklassifikation, -extraktion von Beleginformationen, Matching mit Bankumsätzen, Vorkontierung	Deutschland (EU)	Automatische Finanzbuchhaltung der laufenden Geschäftsvorfälle

Datenkategorien:

- Belegdaten (Rechnungen, Quittungen)
- Bankumsätze

- Stammdaten (Kunden, Lieferanten) - nur soweit auf Belegen enthalten

Vertrag: AVV gemäß Art. 28 DSGVO geschlossen
Besonderheiten: KI verarbeitet nur Dokumente, keine direkten Personendaten außerhalb der Belege

---

3. E-Mail-Versand / Kommunikation

Unterauftragsverarbeiter	Leistung	Standort	Zweck
[Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland]	E-Mail-Infrastruktur	EU (Datenspeicherung in EU-Rechenzentren)	Versand von Rechnungen, Auswertungen, Kommunikation mit Mandanten

Datenkategorien:

- E-Mail-Adressen
- Kommunikationsinhalte (Rechnungen, BWAs als Anhänge)

Vertrag: AVV gemäß Art. 28 DSGVO über Standard-Business-Vertrag

---

4. Backup-Dienstleister

Unterauftragsverarbeiter	Leistung	Standort	Zweck
[Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland]	Datensicherung, Backup-Storage	Deutschland (EU)	Tägliche Backups zur Disaster Recovery

Datenkategorien: Alle im Anhang II genannten personenbezogenen Daten (vollständige Kopie)
Vertrag: AVV gemäß Art. 28 DSGVO geschlossen

---

5. Zahlungsdienstleister

Unterauftragsverarbeiter	Leistung	Standort	Zweck
[OLINDA SAS, 18 rue de Navarin, 75009 Paris (Frankreich) SIRET: 819 489 626 00047]	Zahlungsabwicklung (SEPA-Lastschrift, Kreditkarte)	EU	Einzug der monatlichen Vergütung vom Mandanten

Datenkategorien:

- Name des Mandanten
- Bankverbindung (IBAN)
- Rechnungsbeträge

Vertrag: Standard-AVV des Zahlungsdienstleisters

Besonderheit: Verarbeitet nur Zahlungsdaten des Mandanten selbst, nicht dessen Kundendaten

---