

Annex: Allgemeine Vertragsbedingungen zur Auftragsverarbeitung nach Art. 28 DSGVO der BoonWeb GmbH, Ringstr. 26, 84416 Taufkirchen (Vils) (im Folgenden „BoonWeb GmbH“) für die Nutzung der Online-Plattform rechnungszeug.de

1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1 Die BoonWeb GmbH stellt ihren Kunden (nachfolgend „Auftraggeber“) eine Software zur Rechnungslegung zur Verfügung, in der der Auftraggeber neben eigenen Daten auch Daten von Dritten (Drittdaten) einpflegen kann. Soweit die BoonWeb GmbH diese Daten als Auftragnehmer im Sinne von Art. 28 DSGVO verarbeitet, gelten für diese Verarbeitungstätigkeiten die vorliegenden Allgemeinen Vertragsbedingungen zur Auftragsverarbeitung (nachfolgend „AVB“).

1.2 Im Rahmen der Auftragsverarbeitung verarbeitet BoonWeb GmbH insbesondere folgende Datenkategorien:

- Namen
- Adressen
- Kontaktdaten (E-Mail-Adresse, Telefonnummer etc.)
- Sonstige personenbezogene Daten von Dritten, die der Anwender in das Rechnungserstellungssystem einpflegt

1.3 Von der Auftragsverarbeitung sind insbesondere folgende Personenkategorien betroffen:

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers
- Ansprechpartner der Kunden des Auftraggebers
- Sonstige Dritte, deren personenbezogene Daten der Anwender im Rechnungsetstellungssystem einpflegt

1.4 Die Verarbeitung der Daten durch BoonWeb GmbH findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

2. Laufzeit und Kündigung

Die Laufzeit der Auftragsverarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Soweit und solange nach Beendigung des Hauptvertrags personenbezogene Daten des Auftraggebers im Auftrag weiterverarbeitet werden, gilt diese Vereinbarung bis zu dem Zeitpunkt, zu dem die Verarbeitung dieser Daten durch die BoonWeb GmbH endet. Das Recht auf außerordentliche fristlose Kündigung aus wichtigem Grund bleibt hiervon unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. BoonWeb GmbH zu. BoonWeb GmbH informiert den Auftraggeber unverzüglich, falls BoonWeb GmbH der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit BoonWeb GmbH substantiiert anzweifelt, ist BoonWeb GmbH berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass BoonWeb GmbH durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

3.2 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine Weisung in Textform erfolgen konnte. BoonWeb GmbH hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

4. Kontrollbefugnisse des Auftraggebers

- 4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb von BoonWeb GmbH nicht mehr als erforderlich beeinträchtigen.
- 4.2 Die Ergebnisse der Kontrollen und Weisungen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten von BoonWeb GmbH

- 5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch BoonWeb GmbH erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt BoonWeb GmbH dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- 5.2 BoonWeb GmbH hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

BoonWeb GmbH hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in **Anlage 1** dieser AVB festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt. BoonWeb GmbH wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen.

7. Unterstützungspflichten von BoonWeb GmbH

BoonWeb GmbH wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. BoonWeb GmbH wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die BoonWeb GmbH zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

- 8.1 BoonWeb GmbH ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse von BoonWeb GmbH sind diesen AVB abschließend in **Anlage 2** beigelegt. Für die in **Anlage 2** aufgezählten Subunternehmer gilt die Zustimmung mit Vereinbarung dieser AVB als erteilt.
- 8.2 Beabsichtigt BoonWeb GmbH den Einsatz weiterer Subunternehmer, wird BoonWeb GmbH dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des / der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des / der Subunternehmer(s) als genehmigt. In dringenden Fällen (z.B. bei kurzfristig benötigten Fehleranalysen oder Mängelbeseitigungen), kann BoonWeb GmbH die Anzeige- und Widerspruchsfrist für Subunternehmer angemessen verkürzen. Erfolgt ein fristgerechter Widerspruch, dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und / oder sonstige berechnete Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.
- 8.3 Subunternehmer werden von BoonWeb GmbH unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter (BoonWeb GmbH) und

Unterauftragsverarbeiter (Subunternehmerverträge) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche BoonWeb GmbH zur Ausübung von geschäftlichen Tätigkeiten in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen sowie sonstige Maßnahmen, welche die Vertraulichkeit und / oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. BoonWeb GmbH wird jedoch auch bei diesen Dritteleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

- 8.4 Sämtliche Verträge zwischen BoonWeb GmbH und dem Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieser AVB und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.
- 8.5 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten von BoonWeb GmbH

- 9.1 Verstöße gegen diese AVB, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom BoonWeb GmbH selbst, einer bei BoonWeb GmbH angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die BoonWeb GmbH zur Erfüllung vertraglicher Pflichten eingesetzt hat, begangen wurde.
- 9.2 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter BoonWeb GmbH um Auskunft, Berichtigung oder Löschung von Daten, die BoonWeb GmbH als Auftragsverarbeiter verarbeitet wird BoonWeb GmbH die Anfrage unverzüglich an den Auftraggeber weiterleiten und das weitere Vorgehen mit ihm abstimmen.
- 9.3 BoonWeb GmbH wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von denen auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat BoonWeb GmbH den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung des Hauptvertrags hat BoonWeb GmbH alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine rechtliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

BoonWeb GmbH ist unbefristet und über das Ende des Hauptvertrags hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. BoonWeb GmbH verpflichtet sich, Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit bei BoonWeb GmbH aufnehmen.

12. Schlussbestimmungen

- 12.1 Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist der Sitz von BoonWeb GmbH Gerichtsstand für alle Streitigkeiten aus diesen AVB, sofern insoweit hierfür ein ausschließlicher Gerichtsstand nicht begründet wird.
- 12.2 Soweit personenbezogene Daten im Auftrag betroffen sind, gehen die Regelungen dieser AVB gegenüber den Regelungen der Hauptvereinbarung vor.
- 12.3 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.
- 12.4 BoonWeb GmbH ist berechtigt, die vorliegenden AVB aus sachlich gerechtfertigten Gründen (z.B. Änderungen in der Rechtsprechung, Gesetzeslage, Marktgegebenheiten oder der Geschäfts- oder

Unternehmensstrategie) und unter Einhaltung einer angemessenen Frist zu ändern. Bestandskunden werden hierüber spätestens zwei Wochen vor Inkrafttreten der Änderung per E-Mail benachrichtigt. Sofern der Bestandskunde nicht innerhalb der in der Änderungsmitteilung gesetzten Frist widerspricht, gilt seine Zustimmung zur Änderung als erteilt. Im Falle des Widerspruchs ist BoonWeb GmbH berechtigt, den Vertrag zum Zeitpunkt des Inkrafttretens der Änderung außerordentlich zu kündigen. Die Benachrichtigung über die beabsichtigte Änderung dieser Nutzungsbedingungen wird auf die Frist und die Folgen des Widerspruchs oder seines Ausbleibens hinweisen.

Anlage 1 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

BoonWeb GmbH setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

1. Sicherung der Arbeitsstätte des Auftragsverarbeiters (Zutrittskontrolle)

Die Arbeitsstätte des Auftragnehmers wird in folgender Weise gegen Einbruch und sonstige unbefugte Zutritte gesichert:

- Manuelles Schließsystem / Türschlösser
- Sicherheitsschlösser

- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal

2. Sicherung der IT-Systeme des Auftragsverarbeiters (Zugangskontrolle)

Die IT-Systeme des Auftragsverarbeiters werden in folgender Weise gegen unbefugte Zugriffe (z.B. Hackerangriffe) gesichert:

- Passwortvergabe
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- Erstellen von Benutzerprofilen in den IT-Systemen
- Login in die IT-Systeme mit individuellem Benutzernamen und Passwort
- Zugriffsregeln für Benutzer / Benutzergruppen in den IT-Systemen (Berechtigungskonzept)
- Verwaltung der Berechtigungen durch Systemadministratoren
- Anzahl der Systemadministratoren ist auf das „Notwendigste“ reduziert
- regelmäßige und anlassbezogene Aktualisierung und Überprüfung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)

- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Einsatz von Intrusion-Detection-Systemen

- Festplattenverschlüsselung
- Verschlüsselung mobiler Datenträger (Handys, Laptops etc.)
- Verschlüsselung externer Datenträger (externe Festplatten, USB-Sticks etc.)
- Verschlüsselung der Datensicherungssysteme

- Abschließbarer Serverschrank
- Sichere Aufbewahrung von Datenträgern

3. Protokollierung von Datenverarbeitungsprozessen (Eingabekontrolle)

Folgende Maßnahmen stellen sicher, dass der Auftragsverarbeiter jederzeit erkennen kann, welche Datenverarbeitungsprozesse in seinen Datenverarbeitungssystemen stattgefunden haben (z.B. Eingabe, Veränderung, Sperrung oder Löschung):

- Protokollierung von Zugriffen auf die IT-Systeme des Auftragsverarbeiter (Log-Protokolle)
- Protokollierung von Eingaben, Änderungen und Löschungen (Log-Protokolle)
- Protokollierung der Aktionen einzelner Nutzer

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

4. Sichere Löschung von Daten

Folgende Maßnahmen stellen die ordnungsgemäße Löschung der vertragsgegenständlichen Daten sicher:

- Löschkonzept
- ordnungsgemäße Vernichtung von ausgemusterten Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern (mindestens Stufe P-4)
- ordnungsgemäße Bereinigung von Datenträgern vor Wiederverwendung

5. Datenschutz bei den Subunternehmern des Auftragnehmers

Folgende Maßnahmen stellen sicher, dass sich die vom Auftragnehmer ausgewählten Subunternehmer datenschutzkonform verhalten:

- Auswahl der Subunternehmer unter Sorgfaltsgesichtspunkten (insb. hinsichtlich Datensicherheit)
- Abschluss von DSGVO-konformen Auftragsverarbeitungsverträgen mit dem Subunternehmer
- laufende und anlassbezogene Prüfung des Subunternehmers
- Sicherstellung der Vernichtung der Daten beim Subunternehmer nach Beendigung des Auftrags
- Vereinbarung von Vertragsstrafen bei Verstößen

6. Sicherung von Daten bei Transport und Übermittlung (Weitergabekontrolle)

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) vor unbefugten Dritten geschützt werden:

- Einsatz von VPN-Tunneln
- Verschlüsselung des E-Mail-Verkehrs
- Verschlüsselung der sonstigen Kommunikationswege
- Verschlüsselung physischer Datenträger beim Transport

7. Datensicherung und Backups (Verfügbarkeit und Wiederherstellbarkeit)

Folgende Maßnahmen stellen sicher, dass die vertragsgegenständlichen Daten jederzeit verfügbar sind:

- Backup- & Wiederherstellungskonzept
- Testen der Datenwiederherstellung
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Sicherung der Serverräume
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierung der Serverräume
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Serverräume nicht unter sanitären Anlagen

8. Sonstige Datenschutzmaßnahmen

Folgende weitere Datenschutzmaßnahmen wurden implementiert:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)

- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- Trennung von Produktiv- und Testsystem
- interne Verhaltensregeln
- Risikoanalysen
- Datenschutz-Folgenabschätzung
- Datensicherheitskonzept
- Wiederanlaufkonzept
- Pseudonymisierung
- Zertifikate (z.B. ISO 27001)

9. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	Beschreibung der Leistung	Land der Leistungserbringung
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Bereitstellung von Cloud-Servern und zugehörigen Dienstleistungen	Deutschland