Vereinbarung zur Auftragsverarbeitung

Vertragspartner

Diese Vereinbarung regelt die Verarbeitung von Daten im Auftrag zwischen

Firma _____

Inhaber/Geschäftsführer _____

Straße und Hausnummer _____

PLZ & Ort _____

(im Folgenden auch „Kunde“, „Auftraggeber“)

und der Firma

BuchhaltungsButler GmbH
vertreten durch den Geschäftsführer Maximilian Zielosko
Rheinsberger Str. 76/77
10115 Berlin

(im Folgenden auch „BHB“, „Auftragnehmer“).

Gegenstand und Dauer des Auftrags

Der Gegenstand und die Dauer des Auftrags ergeben sich aus der Leistungsvereinbarung, welche der Kunde mit BHB geschlossen hat (der Hauptvertrag).

Umfang, Art und Zweck des Auftrags

Art und Zweck der Verarbeitung personenbezogener Daten ergeben sich aus dem Hauptvertrag, welche der Kunde mit BHB geschlossen hat.

Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Verarbeitung oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Art der personenbezogenen Daten

BHB verarbeitet im Auftrag des Kunden u.a. Kontodaten, Transaktionsdaten, Bankverbindungsdaten, Kontostände, Buchungsdaten, Rechnungsdaten, Belegdaten, Unternehmens- bzw. Nutzer- bzw. steuerliche Stammdaten sowie weitere Daten, welche der Kunde in die Anwendung von BHB hochlädt.

Kreis der Betroffenen

Vertragsgegenstand ist die Verarbeitung von Daten der Finanzbuchhaltung, welche BHB im Auftrag für den Kunden verarbeitet. Der Kreis der Betroffenen erweitert sich über das Unternehmen, welches der Auftraggeber vertritt, hinaus, sofern der Auftraggeber Daten (z.B. Rechnungen, Abrechnungen o.ä.) z.B. seiner Mitarbeiter, Lieferanten, Kunden, Partner, Gesellschafter, Mitunternehmer o.ä. durch BHB verarbeiten lässt.

Technische und organisatorische Maßnahmen

Die als Anlage beigefügte Beschreibung der technischen und organisatorischen Maßnahmen werden Teil dieser Vereinbarung. Die hier festgelegten Maßnahmen müssen die personenbezogenen Daten vor der zufälligen oder unrechtmäßigen Zerstörung, vor dem zufälligen Verlust, der unberechtigten Änderung oder Weitergabe oder dem unberechtigten Zugang schützen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren, insoweit nicht gesetzliche Regelungen, etwa Aufbewahrungsfristen, diesem entgegenstehen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer diesen Antrag unverzüglich an den Auftraggeber weitergeben.

Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

Zum Ansprechpartner für den Datenschutz wurde Herr Maximilian Zielosko, Rheinsberger Str. 76/77, 10115 Berlin bestellt.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die

Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in der Anlage).

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(6) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse.

(9) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Personen durch die Zurverfügungstellung einer Volltextsuche, um Transaktionen betroffener Personen zu filtern und auszugeben.

(10) Der Auftragnehmer unterstützt unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten.

Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

a) ABBYY Europe GmbH, Landsberger Str. 300, 80687 München. Leistung: Bild-/Texterkennung
b) Bayerische Landesamt für Steuern, Dienststelle München, 80284 München. Leistung: Elster-Schnittstelle, Übermittlung u.a. der UmSt.-Voranmeldung
c) Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxemburg. Leistung: Hosting
d) Userlane GmbH, Georgenstr. 39, 80779 München. Leistung: Nutzer Software-Onboarding
e) Groove Networks LLC, 2 Dearborn St. Newport, RI, USA. Leistung: In-App Wissensdatenbank (FAQ)
f) UserReport (AudienceProject Aps), Ryesgade 3F, 3 floor, 2200 Kopenhagen, Dänemark. Leistung: In-App Feature-Request Portal
g) Wootric, Inc., 220 27th St., San Francisco, CA 94131, USA. Leistung: In-App Umfrage zur Kundenzufriedenheit
h) Zoho Corporation, 4141 Hacienda Drive, Pleasanton, Kalifornien 94588, USA. Leistung: CRM/ERP
I) Google LLC (G Suite), 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Leistung: E-Mail/Cloudstorage

Weitere Informationen zu Art und Umfang der Unterauftragsverhältnisse, auch zu Nebenleistungen, finden Sie in unseren Datenschutzbestimmungen.

(3) Der Auftragnehmer hat die Befugnis, bestehende Unterauftragnehmer zu ersetzen oder neue Unterauftragnehmer zu beauftragen, sofern dies im Einzelfalls notwenig ist. Die Beauftragung eines neuen Unterauftragnehmers ist dem Auftraggeber im Vorhinein anzuzeigen, woraufhin der Auftraggeber ein Widerspruchsrecht hat. Übt der Auftraggeber sein Widerspruchsrecht aus so hat der Auftragnehmer zur Wahrung seiner Interessen das Recht, den Hauptvertrag mit dem Auftragnehmer zu kündigen.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an weitere Unterauftragnehmer sowie dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit dadurch sicher, dass die Verarbeitung der personenbezogenen Daten ausschließlich im Rahmen eines Programms erfolgt, dem von der EU-Kommission ein angemessenes Schutzniveau bescheinigt wurde, z.B. das EU-U.S. Privacy Shield.

Kontrollrechte des Auftragnehmers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
- ein anderes, den gesetzlichen Anforderungen genügendes Dokument (z.B. aktualisierte Beschreibung der umgesetzten technischen und organisatorischen Maßnahmen).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer erstattet dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

(2) Dem Auftragnehmer sind die geltenden datenschutzrechtlichen Melde- bzw. Benachrichtigungspflichten gegenüber Aufsichtsbehörden und Betroffenen, insbesondere deren zeitliche und inhaltliche Vorgaben, bekannt. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.

(3) Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Melde- bzw. Benachrichtigungspflichten treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

(4) Der Auftragnehmer hat etwaige Verstöße, einschließlich aller hiermit im Zusammenhang stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen, entsprechend der jeweils geltenden Datenschutzvorschriften zu dokumentieren. Die Dokumentation ist dem Auftraggeber auf Aufforderung unverzüglich herauszugeben.

Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen

Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, insoweit dem nicht gesetzliche Regelungen, etwa Aufbewahrungsfristen, entgegenstehen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Sonstiges

Die Regelungen dieser Vereinbarung gelten auch nach einer Beendigung des Hauptvertrages bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten des Auftragnehmers an den Auftraggeber fort.

Im Übrigen gelten die Bestimmungen des Hauptvertrages entsprechend.

_____	_____
(Ort, Datum)	(Unterschrift Auftraggeber)
_____	_____
(Ort, Datum)	(Unterschrift Auftragnehmer)

Anlage: Technische und organisatorische Maßnahmen

Vertraulichkeit

1. Zutrittskontrolle

Besucher können nur in Begleitung von Co-Workern und zu den Geschäftszeiten (Mo-Fr, 08:00 – 21:00 Uhr) die Geschäftsräume unter Aufsicht betreten. Zum Eintritt ist eine Schlüssel-App bzw. eine Chipkarte für den Check-In notwendig. Ein Empfang beaufsichtigt den Eintritt in die Geschäftsräume. Die Geschäftsräume sind durch eine Alarmanlage geschützt.

Für das Rechenzentrum gelten die IT-Sicherheitsrichtlinien des jeweiligen Betreibers.

2. Zugangskontrolle

Die Rechner der Mitarbeiter sind mit einer Firewall und Virenscannern geschützt. Die Entsperrung der Computer ist nur mittels Passwort möglich. Beim Verlassen des Arbeitsplatzes sind die Arbeitscomputer zu sperren. Zugriff zu den Systemen (etwa CRM, Rechnungsstellung, Mailing o.ä.) erfolgt nur mittels sicherer und individueller Passwörter, welche verschlüsselt im Passwortmanager Keepass aufbewahrt werden.

Der Server zur Verarbeitung der Kundendaten unterliegen speziellen Schutzmaßnahmen. Der Zugang zum System kann nur durch ein komplexes Passwort, welches regelmäßig geändert wird, sowie über bestimmte IP Adressen und Ports erfolgen. Das „Root“ Passwort ist nur den Gesellschaftern, dem Head of Backend sowie dem Server-Administrator bekannt.

3. Zugriffskontrolle

Sämtliche Zugriffe auf Buchhaltungsdaten sind nur einem stark eingeschränkten Personenkreis technisch möglich. Wenngleich ein Datenzugriff technisch möglich ist, erfolgt niemals eine Einsichtnahme in Buchungsdaten des Auftraggebers, es sei denn, der Auftraggeber erteilt eine explizite Weisung um Änderungen, Löschungen o.ä. am Datenbestand vorzunehmen.

Andere Mitarbeiter des Unternehmens haben keinen Zugriff auf die Verarbeitungssysteme des Unternehmens, mit Ausnahme der Stammdaten des Auftraggebers (Name, Firmierung, Adresse, Kontaktdaten, gebuchte Dienstleistung).

4. Trennungsgebot

Daten, welche zu unterschiedlichen Zwecken erhoben und verarbeitet werden, werden getrennt voneinander gespeichert und verarbeitet. Jeder Kunde hat seinen eigenen Kundenzugang. White-Label-Instanzen nutzen zudem physisch getrennte Server.

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Bei Datenanalysen werden die Daten pseudonymisiert und anonym verarbeitet.

Integrität

6. Weitergabekontrolle

Werden Daten weitergeleitet, werden diese mit modernsten Verschlüsselungstechnologien (z.B. SSL, https) geschützt soweit dieses technisch möglich und wirtschaftlich vertretbar ist.

7. Eingabekontrolle

Durch eine Nutzerverwaltung ist es möglich, die Eingabe von Daten einem Nutzer zuzuordnen. Zudem wird in den Logfiles Datum und Uhrzeit der Eingabe sowie in manchen Fällen auch die IP-Adresse gespeichert.

Verfügbarkeit und Belastbarkeit

8. Verfügbarkeitskontrolle

Die Stromversorgung und Netzersatzanlage garantieren höchste Ausfallsicherheit. Die unmittelbare Stromversorgung des Servers ist typenabhängig, so dass bei der Verwendung entsprechender Typen zusätzlich eine redundante Stromversorgung über ein redundantes Netzteil (2 Netzteile) gewährleistet ist.

Der gesamte Energieverbrauch der Rechenzentren wird über eine unterbrechungsfreie Stromversorgung (USV) sichergestellt. Die USV filtert vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.

Der Schutz vor Viren und Hacker-Angriffen wird durch eine Firewall sowie diverse, manuelle Maßnahmen, welche dem aktuellen Stand der Server-Administration entsprechen, sichergestellt.

Alle Daten werden mindestens einmal täglich auf einem räumlich getrennten Backup-Server gesichert. Backups werden mindestens 6 Wochen vorgehalten.

Für die Einrichtung und Durchführung zusätzlicher Backups der Daten ist der Kunde selbst verantwortlich.

9. Wiederherstellbarkeit

Nach einem etwaigen Datenverlust ist die schnelle Wiederherstellbarkeit von unserem Backup-System gewährleistet.

10. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Ein Datenschutzbeauftragter wurde bestellt. Die Wirksamkeit der Maßnahmen wird u. a. durch den Datenschutzbeauftragten und durch den Informationssicherheitsbeauftragten der BHB laufend geprüft. Der Datenschutzbeauftragte oder von ihm oder der Geschäftsleitung beauftragte Mitarbeiter führen regelmäßig interne Kontrollen der Einhaltung der technischen und organisatorischen Maßnahmen der Datensicherheit durch. Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft. Es erfolgt mindestens jährlich eine technische Überprüfung der Datenverarbeitungssysteme.

Sicherheitsvorfälle werden dokumentiert und ausgewertet. Für die Sicherheitsvorfälle besteht ein geschultes Krisenteam.