VEREINBARUNG

AUFTRAGSDATENVERARBEITUNG

NACH ART. 28 DSGVO

Stand: 12.12.2024

INHALTSVERZEICHNIS

1. PARTEIEN

Diese Vereinbarung über die Verarbeitung von personenbezogenen Daten wird zwischen folgenden Parteien abgeschlossen und ergänzt bestehende Verträge, sofern nicht anders geregelt:

1.1. Verantwortlicher gem. Art. 4 Z 7 DSGVO („Auftraggeber“)

Name	
Straße	
PLZ/Ort	

1.2. Auftragsverarbeiter gem. Art. 4 Z 8 DSGVO („Auftragnehmer“)

BMD SYSTEMHAUS GesmbH
Sierninger Straße 190
A-4400 Steyr

UID-Nr. ATU24168102
LG Steyr, FN 118356d
www.bmd.com

2. GEGENSTAND DIESER VEREINBARUNG: TÄTIGKEITEN

Folgende Dienstleistungen des Auftragnehmers fallen im Sinne der DSGVO unter diese Vereinbarung:

2.1. Supportdienstleistungen vor Ort beim Auftraggeber

Darunter fallen Schulungen zur Einführung der Software beim Auftraggeber und sonstige Leistungen, die vor Ort beim Auftraggeber durchgeführt werden.

2.2. Support mit Fernwartungszugriff

Zur Bearbeitung einer Anfrage des Auftraggebers wird durch den Auftraggeber dem Auftragnehmer ein direkter Zugriff auf das System des Auftraggebers gewährt.

2.3. Support mit Fernzugriff via Software

Zur Bearbeitung einer Anfrage des Auftraggebers wird durch den Auftragnehmer eine Online-Sitzung auf einem Arbeitsplatz des Auftraggebers hergestellt. Der Auftraggeber muss vor Durchführung der Dienstleistung den Zugriff bestätigen, bevor der Bildschirminhalt übertragen wird.

2.4. Fehleranalyse mit Daten des Auftraggebers

Werden zur Fehleranalyse bzw. zur Durchführung von Dienstleistungen Daten des Auftraggebers benötigt, werden diese über einen gesicherten FTP-Server vom Auftraggeber an den Auftragnehmer übermittelt. Ist eine Übermittlung der Daten online nicht möglich, aus welchen Gründen auch immer, kann der Auftraggeber vom Auftragnehmer gegen Kostenersatz einen passwortgeschützten und sicheren Datenträger anfordern (der Auftraggeber übernimmt während des Postweges die Haftung für den Verlust des Datenträgers).

2.5. BMD-Cloud-Service

Nutzt der Auftraggeber die BMD Cloud, so werden je nach Umfang der Beauftragung die Daten des Auftraggebers auf der Hardware des Auftragnehmers gespeichert. Die Speicherung der Daten erfolgt dabei ausschließlich innerhalb des EWR (gem. Kapitel 5 DSGVO). Nähere Informationen zu den BMD-Cloud-Nutzungsbedingungen sind im BMD-Cloud-Vertrag enthalten.

3. GEGENSTAND DIESER VEREINBARUNG: DATEN

Folgende Daten werden vom Auftragnehmer elektronisch verarbeitet:

3.1. Daten innerhalb der BMD Applikation

Der Auftragnehmer verarbeitet Daten elektronisch innerhalb der BMD Applikation. Dazu zählen: Finanzbuchhaltung, Lohnverrechnung, Controlling/Kostenrechnung, Bilanz/Anbu/Steuern, CRM, Zeiterfassung, Personalmanagement, Projektmanagement/Leistungserfassung, WWS/Kasse/PPS, Kanzleiverwaltung, Wirtschaftsprüfung.

3.2. Daten außerhalb der BMD Applikation

Der Auftragnehmer verarbeitet Daten, die außerhalb der BMD Applikation gespeichert werden, beispielsweise Buchhaltungs- oder Lohnverrechnungsdaten, die vom Auftraggeber zur Fehleranalyse zur Verfügung gestellt werden. Deren Dokumentenkategorien sind vom Auftraggeber vorgegeben und können nicht seitens des Auftragnehmers beeinflusst werden. Diese Daten sind dem Auftragnehmer auch nicht im Vorhinein bekannt.

4. PFLICHTEN DES AUFTRAGNEHMERS

4.1. Daten und Verarbeitungsergebnisse

Der Auftragnehmer verarbeitet Daten und Verarbeitungsergebnisse nur auf dokumentierte Weisung des Auftraggebers, im Rahmen eines schriftlichen Auftrages bzw. Vertrages mit dem Auftraggeber. Wird der Auftragnehmer von einer Behörde verpflichtet, Daten des Auftraggebers herauszugeben, ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich davon in Kenntnis zu setzen.

4.2. Vertraulichkeit und Verschwiegenheitspflicht

Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sämtliche Mitarbeiterinnen und Mitarbeiter des Auftragnehmers, die mit der Bearbeitung der unter Punkt 2 beschriebenen Tätigkeiten, sowie alle Personen, die mit den damit in Verbindung stehen organisatorischen Tätigkeiten beauftragt werden, sind zur Verschwiegenheit gemäß Art. 28 Abs. 3 DSGVO und § 6 DSG in der geltenden Fassung verpflichtet. Eine gesonderte Verschwiegenheitserklärung kann beim Auftragnehmer angefordert werden.

4.3. Mitteilungs- und Meldepflichten

Im Falle einer Verletzung des Datenschutzes hat der Auftragnehmer den Auftraggeber unverzüglich, jedenfalls innerhalb von 24 Stunden ab Bekanntwerden der Verletzung beim Auftragnehmer, zu informieren. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden, sofern diese in Bezug auf die Daten des Auftraggebers stehen.

4.4. Unterstützung bei den Transparenzpflichten gegenüber betroffenen Personen

Der Auftraggeber kann zur Erfüllung der Transparenzpflichten gegenüber den aus seiner Sicht betroffenen Personen die Unterstützung des Auftragnehmers anfordern. Diese Leistung wird zu den aktuell gültigen Stundensätzen des Auftragnehmers erbracht.

5. DATENSICHERHEIT UND SICHERHEITSMAßNAHMEN

Der Auftragnehmer erklärt rechtsverbindlich, dass er ausreichende technische und organisatorische Sicherheitsmaßnahmen gemäß Art. 32 DSGVO ergriffen hat und diese stets auf dem aktuellen Stand der Technik hält, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Zusätzlich wurde eine Zertifizierung nach ISO 27001 erfolgreich durchgeführt.

5.1. Technische Maßnahmen

5.1.1. Zutrittskontrolle

Die Serverräume des Auftragnehmers sind durch eine Zutrittskontrolle geschützt und können nur von berechtigten Mitarbeiterinnen und Mitarbeitern betreten werden.

5.1.2. Zugriffskontrolle

Alle Systeme sind durch einen umfangreichen Passwortschutz gesichert und unterliegen einem Berechtigungskonzept, welches sicherstellt, dass nur berechtigte Personen Zugriff auf Daten erhalten.

5.1.3. Weitergabekontrolle

Daten werden über sichere Wege übermittelt (z. B. VPN-Verbindung).

5.1.4. Eingabekontrolle

Personenbezogene Daten können nur von berechtigten Personen erfasst, verändert und gelöscht werden. Eingaben in den Kundenstammdaten des Auftragnehmers werden mitprotokolliert.

5.1.5. Auftragskontrolle

Der Auftragnehmer handelt in jenem Umfang, der mit dem Auftraggeber vereinbart wurde (Softwareauftrag, Dienstleistungsanfragen, Wartungsvertrag etc.).

5.1.6. Verfügbarkeitskontrolle

Der Auftragnehmer bestätigt die laufende Durchführung von Datensicherungen sowie die Überwachung seiner Betriebsvoraussetzungen. Im Bedarfsfall stehen Notfallpläne zur Verfügung, um mögliche Ausfälle der Betriebsvoraussetzung möglichst gering zu halten.

5.2. Organisatorische Maßnahmen

5.2.1. Klare Zuständigkeiten

Es sind interne Zuständigkeiten für die Fragen der Datensicherheit definiert.

5.2.2. Verschwiegenheitspflicht der Mitarbeiter/innen

Die Mitarbeiter/innen werden über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere werden Sie dazu verpflichtet, personenbezogene Daten nur auf ausdrückliche Anweisung eines Vorgesetzten an Dritte zu übermitteln.

5.2.3. Schulungen und Informationsmaßnahmen

Die Mitarbeiter/innen werden regelmäßig zu Fragen der Datensicherheit geschult und angemessen über Fragen der Datensicherheit informiert (z. B. Passwortsicherheit). Besonderer Wert wird auf die Schulung und Schärfung des Sicherheitsbewusstseins der Mitarbeiter/innen gelegt.

5.2.4. Geordnete Beendigung des Dienstverhältnisses

Bei Beendigung des Dienstverhältnisses erfolgt eine unverzügliche Sperrung aller Konten des ausscheidenden Mitarbeiters sowie eine Abnahme aller Schlüssel des auscheidenden Mitarbeiters.

5.2.5. Verwaltung von Computer-Hardware

Es werden Aufzeichnungen darüber geführt, welche Endgeräte (z. B. Laptop, Mobiltelefon,…) welchem Mitarbeiter zugewiesen wurden.

5.2.6. Auswahl der Dienstleister

Bei der Auswahl von Dienstleistern wird das vom Dienstleister gebotene Datensicherheitsniveau berücksichtigt. Der Einsatz eines Dienstleisters, der als Auftragsverarbeiter einzustufen ist, erfolgt nur nach Abschluss einer Auftragsverarbeitervereinbarung.

5.2.7. Sichere Datenentsorgung

Papier, welches personenbezogene Daten enthält, wird grundsätzlich geschreddert bzw. einem externen Dienstleister zur sicheren Vernichtung übergeben. Datenträger werden vor ihrer Entsorgung vollständig überschrieben oder physisch zerstört, sodass die darauf gespeicherten Daten nicht wieder hergestellt werden können.

5.3. Weitere präventive Maßnahmen

5.3.1. Erkennung von Sicherheitsverletzungen durch Mitarbeiter/innen

Alle Mitarbeiter/innen werden instruiert, wie sie Sicherheitsverletzungen erkennen können (z. B. Meldungen von Anti-Viren-Software).

5.3.2. Betriebsfremde Personen

Betriebsfremde Personen müssen sich am Empfang registrieren lassen. Betriebsfremden Personen ist das Betreten der Betriebsräumlichkeiten nur in Begleitung einer betriebsangehörigen Person gestattet.

5.3.3. Audits

Es werden regelmäßige Audits, gemäß ISO 9001 und ISO 27001, durchgeführt (z. B. Prüfung, ob alle kritischen Sicherheits-Updates installiert wurden). Insbesondere erfolgt eine regelmäßige Prüfung der erteilten Zugriffs- und Zutrittsberechtigungen (welchem Mitarbeiter ist welcher Benutzer-Account mit welchen Zugriffsrechten zugewiesen,…).

5.3.4. Brandmelder

Es sind Brandmelder installiert, die durch Rauch automatisch ausgelöst werden.

5.4. Reaktive Sicherheitsmaßnahmen

5.4.1. Datensicherung

Es werden regelmäßig Datensicherungen erstellt und diese sicher aufbewahrt.

5.4.2. Meldepflicht für Mitarbeiter/innen

Alle Mitarbeiter/innen sind angewiesen, Sicherheitsverletzungen unverzüglich an eine zuvor definierte interne Stelle bzw. Person zu melden.

5.4.3. Meldepflicht für externe Dienstleister

Allen Dienstleistern wurden Kontaktdaten für die Meldung von Sicherheitsverletzungen mitgeteilt.

5.4.4. Reaktion auf Sicherheitsverletzungen: Adäquater Prozess

Es wird durch einen geeigneten Prozess sichergestellt, dass Sicherheitsverletzungen innerhalb von 72 Stunden ab Kenntnis von der Sicherheitsverletzung an die Datenschutzbehörde gemeldet werden können. Insbesondere sind allen Mitarbeiterinnen und Mitarbeitern die Notfall-Telefonnummern der zu involvierenden Personen bekannt zu geben (z. B. Notfall-Telefonnummer für den IT-Support).

6. RECHTE DES AUFTRAGGEBERS

Der Auftraggeber ist berechtigt, die Einhaltung der Datenschutzvorschriften beim Auftragnehmer in angemessenem Umfang selbst oder durch einen beauftragten Dritten zu überprüfen. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten unentgeltlich zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, die von dem Verantwortlichen oder einem anderen von diesem beauftragen Prüfer durchgeführt werden.

6.1. Recht auf Auskunft (Art. 15 DSGVO)

Der Auftraggeber hat gemäß Art. 15 DSGVO jederzeit das Recht, eine Auskunft über alle beim Auftragnehmer über den Auftraggeber gespeicherten Daten zu beantragen. Die dazu beim Auftragnehmer eingerichtete E-Mail-Adresse lautet: datenschutz@bmd.at.

Im Zweifelsfall kann der Auftragnehmer zusätzliche Informationen zur Bestätigung der Identität des Auftragsgebers einfordern. Sollte der Auftraggeber offenkundig unbegründet oder besonders häufig sein Recht auf Auskunft wahrnehmen, kann ein angemessenes Bearbeitungsentgelt verlangt bzw. die Bearbeitung des Antrages verweigert werden.

6.2. Recht auf Berichtigung (Art. 16 DSGVO)

Verarbeitet der Auftragnehmer personenbezogene Daten, die unvollständig oder fehlerhaft sind, kann der Auftraggeber deren Berichtigung bzw. deren Vervollständigung verlangen.

6.3. Recht auf Löschung (Art. 17 DSGVO)

Der Auftraggeber ist berechtigt, die Löschung seiner Daten beim Auftragnehmer zu verlangen, wenn einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben bzw. verarbeitet wurden, nicht mehr notwendig.
b) Der Auftraggeber widerruft seine Einwilligung und es fehlt eine Rechtsgrundlage für die weitere Verarbeitung/Speicherung.
c) Der Auftraggeber legt Widerspruch gegen die Verarbeitung ein und es liegen keine berechtigten Gründe für die weitere Verarbeitung vor.
d) Die Daten des Auftraggebers wurden unrechtmäßig verarbeitet.

6.4. Recht auf Einschränkung (Art. 18 DSGVO)

Der Auftraggeber kann vom Auftragnehmer die Einschränkung der Verarbeitung verlangen, wenn

a) der Auftraggeber die Richtigkeit der Verarbeitung bestreitet, und zwar für die Dauer, die es dem Auftragnehmer ermöglicht, die Richtigkeit der Daten zu überprüfen.
b) die Verarbeitung der Daten unrechtmäßig ist, der Auftraggeber aber eine Löschung ablehnt.
c) die Daten vom Auftragnehmer für den vorgesehenen Zweck nicht mehr benötigt werden, der Auftraggeber diese Daten aber noch zur Geltendmachung oder Verteidigung von Rechtsansprüchen braucht.
d) der Auftraggeber Widerspruch gegen die Verarbeitung der Daten eingelegt hat.

6.5. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Der Auftraggeber hat das Recht, seine personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, sofern die Daten aufgrund einer Zustimmung des Auftraggebers bzw. zur Erfüllung eines Vertrages vom Auftraggeber gespeichert wurden und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

6.6. Recht auf Widerspruch (Art. 21 DSGVO)

Werden personenbezogene Daten des Auftraggebers aufgrund des Art. 6 Abs. 1 lit. b oder f vom Auftragnehmer verarbeitet, so hat der Auftraggeber jederzeit das Recht auf Widerspruch, sofern kein überwiegendes Schutzinteresse an den Daten besteht. Der Auftraggeber kann der Zusendung von Werbung jederzeit ohne Angabe von Gründen widersprechen.

6.7. Recht auf Beschwerde

Der Auftraggeber hat das Recht auf Beschwerde bei der dafür vorgesehenen Aufsichtsbehörde, wenn er der Meinung ist, dass der Auftragnehmer gegen österreichisches oder europäisches Datenschutzrecht verstößt.

7. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Die Auftragsverarbeitung erfolgt ausschließlich innerhalb des EWR.

8. SUB-AUFTRAGSVERARBEITER

Der Auftraggeber muss der Heranziehung von Sub-Auftragsverarbeitern durch den Auftragnehmer zustimmen. Der Auftragnehmer muss den Einsatz von Sub-Auftragsverarbeitern rechtzeitig an den Auftraggeber kommunizieren. Erfolgt innerhalb von 14 Tagen bzw. bis zur vereinbarten Erbringung einer Dienstleistung kein Einspruch gegen die Heranziehung eines Sub-Auftragsverarbeiters, gilt der Einsatz als durch den Auftraggeber bestätigt. Alle vom Auftragnehmer eingesetzten Sub-Auftragsverarbeiter unterliegen den Verschwiegenheitspflichten gem. Punkt 4.2.

Zu den Sub-Auftragsdatenverarbeitern seitens des Auftragnehmers zählen unter anderem:

- BMD Töchter:
  - BMD GmbH (Deutschland)
  - BMD Schweiz AG
  - BMD Rendszerház Kft. (Ungarn)
  - BMD Business Solutions s.r.o. (Slowakei)
- Zertifizierte VorOrtPartner, die qualifiziert sind, Schulungen im Auftrag des Auftragnehmers durchzuführen und Support zu leisten. Deren Einsatz wird durch die Auftragserteilung des Auftraggebers zugestimmt.
- Externe Fachtrainer/innen (führen Seminare durch). Deren Einsatz wird durch die Anmeldung zum jeweiligen Seminar zugestimmt.
- Reisswolf Österreich GmbH (führt die Vernichtung der Datenträger und der Akten durch)
- Energie AG Oberösterreich Umwelt Service GmbH Steyr (führt die Vernichtung der Akten durch)
- GoTo Technologies Ireland Unlimited Company (Software für die Verwendung der Fernwartung; Verarbeitung innerhalb des EWR kann nicht gewährleistet werden)
- Microsoft Azure (bei Verwendung der BMD Cloud)
- VirtualQ GmbH (bei Verwendung des Rückrufservices für Support-Hotline)
- Dynatrace Austria GmbH (bei Verwendung von BMD Web Applikationen)
- Xortex eBusiness GmbH (Software für Versand des Info-Newsletters)
- Mailworx Eworx Network & Internet GmbH (Software für Versand des Akademie-Newsletters)
- GLS Austria GmbH (Versand von Paketen)
- Flexdoc GRZ IT Center Linz GmbH (Versand von Briefen)

Den oben angeführten Sub-Auftragsverarbeitern wird durch Unterschrift des Vertrages zugestimmt.

9. DAUER DER VEREINBARUNG

Die Dauer der Auftragsdatenverarbeitungsvereinbarung ist an die Dauer des Hauptvertrages gebunden und endet daher mit dessen Wegfall. Der Auftragnehmer ist nach Beendigung der Dienstleistung verpflichtet, dem Auftraggeber alle Verarbeitungsergebnisse und Unterlagen, die Daten des Auftraggebers erhalten, zu übergeben bzw. in seinem Auftrag unwiederbringlich zu vernichten, soweit nicht im Einzelfall gesetzliche Bestimmungen oder behördliche Anforderungen einer solchen Vernichtung entgegenstehen.

10. SCHLUSSBESTIMMUNGEN

Änderungen und Ergänzungen zu dieser Vereinbarung bedürfen der Schriftform. Es bestehen keine mündlichen Nebenabreden. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Für Streitigkeiten aus dieser Vereinbarung gilt österreichisches Recht, Gerichtsstand ist Steyr.

11. UNTERSCHRIFTEN

11.1. Auftraggeber

Kontaktperson	
Funktion	
Unterschrift	
Datum, Ort	

11.2. Auftragnehmer

Kontaktperson	
Funktion	
Unterschrift	
Datum, Ort	