

Vereinbarung zur Auftragsverarbeitung

als Anlage zum Vertrag / zur Leistungsbeschreibung vom _____
- nachfolgend „Leistungsvereinbarung“ -

zwischen

_____, vertreten durch _____
- nachfolgend „Verantwortlicher“ -

und

BISS Software GmbH, vertreten durch ihren Geschäftsführer/in
- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -
wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel

§ 1 Anwendungsbereich

§ 2 Konkretisierung des Auftragsinhalts

§ 3 Verantwortlichkeit und Weisungsbefugnis

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

§ 7 Löschung und Rückgabe von Daten

§ 8 Datenschutzkontrolle

§ 9 Schlussbestimmungen

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungs-
verhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den
Vorgaben der europäischen Datenschutz-Grundverordnung (*Verordnung (EU) 2016/679 des
Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der
Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie
95/46/EG - DSGVO*), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren,
schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

§ 2 Konkretisierung des Auftragsinhalts

- (1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung.
- (2) Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter: Die Datenarten und -kategorien ergeben sich aus und richten sich nach den Inhalten der Leistungsvereinbarung (z.B. Softwarepflege, Hotline, Wartung).
- (3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist auf die Mitarbeiter des Auftragsverarbeiters beschränkt.

§ 3 Verantwortlichkeit und Weisungsbefugnis

- (1) Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.
- (2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.
- (3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.
- (4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.
- (5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigte Person auf Seiten des Verantwortlichen ist deren Geschäftsführer/in oder _____.
Die zum Empfang berechtigte Person auf Seiten des Auftragsverarbeiters ist deren Geschäftsführer/in.
- (6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(8) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt. Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums ist nur zulässig wenn sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird und bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig bei der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Der Datenschutzbeauftragte des Auftragsverarbeiters ist deren Geschäftsführer/in. Die Kontaktdaten der/des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den

Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich unter angemessener Voranmeldung jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(6) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

(7) Für etwaige im Zusammenhang mit § 5 vom Verantwortlichen veranlasste auf Seiten des Auftragsverarbeiters anfallende Arbeitszeit oder Aufwände, kann der Auftragsverarbeiter vom Verantwortlichen angemessene Vergütung verlangen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag unter angemessener Voranmeldung jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht (hier: die/der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) und der Kontrolle durch die/den Datenschutzbeauftragten des Verantwortlichen mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftrags Erfüllung

haben. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt. Für etwaige in diesem Zusammenhang anfallende Aufwände oder Arbeitszeit kann der Auftragsverarbeiter vom Verantwortlichen angemessene Vergütung verlangen.

§ 9 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Datum, Ort

Datum, Ort

Unterschrift (Verantwortlicher)

Unterschrift (Auftragsverarbeiter)

Name, Vorname, Funktion

Name, Vorname, Funktion

Anhang „Technisch-organisatorische Maßnahmen“

zur Vereinbarung zur Auftragsverarbeitung vom _____

zwischen _____

und der BISS Software GmbH

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Dies erfolgt z.B. durch Schlüssel oder ein Zutrittskontrollsystem.

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies erfolgt z.B. durch Kennwortverfahren oder Einrichtung eines Benutzerstammsatzes pro User.

3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies erfolgt z.B. durch bedarfsorientierte Ausgestaltung des Berechtigungskonzepts oder der Zugriffsrechte.

4. Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Dies erfolgt z.B. durch Maßnahmen bei Transport und Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

5. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies erfolgt z.B. durch Protokollierung oder Auswertungssysteme, die die Nachvollziehbarkeit der Datenverwaltung gewährleisten.

6. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können. Dies erfolgt z.B. durch Abgrenzen der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter durch eindeutige Vertragsgestaltung.

7. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies erfolgt z.B. durch Backup-Verfahren, unterbrechungsfreie Stromversorgung, Firewall.

8. Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies erfolgt z.B. durch Mandantenfähigkeit oder Funktionstrennung zwischen Produktion/Test.

Datum, Ort

Datum, Ort

Unterschrift (Verantwortlicher)

Unterschrift (Auftragsverarbeiter)

Name, Vorname, Funktion

Name, Vorname, Funktion