

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

gemäß Art. 28 DSGVO

Stand: 19. August 2026

Vertragsparteien

Auftraggeber – Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO

Firma / Organisation: _____

Straße, Hausnummer: _____

PLZ, Ort: _____

Vertreten durch: _____

E-Mail: _____

Telefon: _____

Kundennummer: _____

– nachfolgend „Auftraggeber“ –

Auftragnehmer – Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO

bmp GmbH

Eichendorffstr. 14

31224 Peine

Deutschland

Telefon: +49 5172 94980-0

E-Mail: mail@bmpgmbh.de

Vertreten durch die Geschäftsführer Erik Böker und Kai Magerkord

Amtsgericht Hildesheim, HRB 101372

– nachfolgend „Auftragnehmer“ –

– gemeinsam die „Parteien“ –

Präambel

Der Auftraggeber nutzt Leistungen des Auftragnehmers aus den Bereichen Softwareentwicklung, Webhosting und Betreuung. Dabei erhält der Auftragnehmer Zugang zu personenbezogenen Daten, für die der Auftraggeber Verantwortlicher ist. Für diese Fälle regelt dieser Vertrag die Rechte und Pflichten der Parteien nach Art. 28 DSGVO.

Der Vertrag erfasst drei Leistungsbereiche, die einzeln oder gemeinsam beauftragt werden können. Welche Bereiche gelten, ergibt sich aus **Anlage 1 Ziffer 1**:

- **Bereich A – Webhosting und Betrieb:** Der Auftragnehmer betreibt die Website oder Anwendung des Auftraggebers auf von ihm bereitgestellter Infrastruktur. Er verarbeitet damit **laufend** alle personenbezogenen Daten, die über dieses System verarbeitet werden.

- **Bereich B – Betreuung, Wartung und Fernwartung:** Zugang zu personenbezogenen Daten entsteht **anlassbezogen**, wenn der Auftraggeber Unterstützung anfordert und den Zugriff freigibt.
- **Bereich C – Entwicklung, Datenübernahme und Test mit Echtdaten:** Der Auftraggeber stellt dem Auftragnehmer produktive Datenbestände zur Verfügung, damit dieser sie übernehmen, prüfen oder eine Entwicklung daran erproben kann. Die Verarbeitung ist auf den jeweiligen Vorgang begrenzt.

Dieser Vertrag ergänzt den zwischen den Parteien bestehenden Vertrag über die Hauptleistung (nachfolgend „Hauptvertrag“). Er begründet keine eigenständige Leistungspflicht.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers, soweit sie im Zusammenhang mit den in Anlage 1 beschriebenen Leistungen erfolgt.

(2) Der Auftragnehmer verarbeitet die Daten ausschließlich zu den in Anlage 1 genannten Zwecken. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers – insbesondere zu Werbe-, Analyse- oder Produktentwicklungszwecken – findet nicht statt.

(3) Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Er endet automatisch mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf.

(4) Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Der Bestand des Hauptvertrages bleibt hiervon unberührt.

(5) Die Verarbeitung findet in der Bundesrepublik Deutschland und im Übrigen innerhalb der Europäischen Union statt. Die Infrastruktur für Bereich A wird bei der Hetzner Online GmbH in Deutschland betrieben (siehe Anlage 3).

(6) Für die Kommunikation mit dem Auftraggeber setzt der Auftragnehmer Microsoft 365 ein (siehe Anlage 3). Microsoft speichert und verarbeitet die Daten nach der EU-Datengrenze innerhalb der Europäischen Union. Ein Zugriff aus den Vereinigten Staaten ist im Rahmen von Support- und Wartungsvorgängen nicht vollständig auszuschließen; Grundlage hierfür sind der Angemessenheitsbeschluss der Europäischen Kommission vom 10. Juli 2023 (EU-U.S. Data Privacy Framework), unter dem die Microsoft Corporation zertifiziert ist, sowie ergänzend die Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO als Bestandteil des Microsoft Data Protection Addendum.

(7) Eine darüber hinausgehende Verarbeitung in einem Drittland erfolgt nicht und bedürfte der vorherigen Zustimmung des Auftraggebers in Textform sowie der Einhaltung der Voraussetzungen der Art. 44 bis 49 DSGVO.

§ 2 Konkretisierung des Auftragsinhalts

Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen ergeben sich abschließend aus **Anlage 1**, die Bestandteil dieses Vertrages ist.

§ 3 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Dies gilt auch für die Übermittlung von Daten an ein Drittland oder eine internationale Organisation, es sei denn, der Auftragnehmer ist hierzu nach dem Recht der Union oder der Mitgliedstaaten verpflichtet; in diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Weisungen werden in Textform erteilt. Mündliche Weisungen – etwa im Verlauf einer Fernwartungssitzung – sind zulässig; sie sind vom Auftraggeber unverzüglich in Textform zu bestätigen. Erfolgt keine Bestätigung, dokumentiert der Auftragnehmer die Weisung selbst und teilt sie dem Auftraggeber mit.

(3) Der Auftraggeber trägt die Verantwortung für die Rechtmäßigkeit der von ihm erteilten Weisungen sowie für die Zulässigkeit der Verarbeitung insgesamt.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen (Art. 28 Abs. 3 Satz 3 DSGVO). Er ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis der Auftraggeber sie bestätigt oder ändert.

(5) Weisungsberechtigt auf Seiten des Auftraggebers sind die in **Anlage 1 Ziffer 9** benannten Personen; weisungsempfangend sind die dort benannten Personen des Auftragnehmers. Änderungen sind der jeweils anderen Partei unverzüglich mitzuteilen.

§ 4 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich:

- 1 personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers zu verarbeiten;
- 2 innerhalb seines Verantwortungsbereichs die Sicherheit der Verarbeitung nach Art. 32 DSGVO durch die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen zu gewährleisten;
- 3 sicherzustellen, dass sich alle mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO) und über die einschlägigen Datenschutzbestimmungen unterrichtet sind;
- 4 den Auftraggeber unverzüglich zu informieren, wenn er einen Verstoß gegen den Schutz personenbezogener Daten des Auftraggebers feststellt (§ 8 dieses Vertrages);
- 5 den Auftraggeber bei der Erfüllung von Betroffenenrechten sowie bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen zu unterstützen (§ 9 dieses Vertrages);
- 6 ein Verzeichnis aller Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO zu führen und dem Auftraggeber auf Anforderung den ihn betreffenden Auszug in Textform zur Verfügung zu stellen;
- 7 dem Auftraggeber alle Informationen zur Verfügung zu stellen, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind, und diese Informationen auf Anforderung in Textform zu übermitteln;
- 8 die Verarbeitung räumlich, organisatorisch oder logisch von Verarbeitungen für andere Auftraggeber zu trennen;
- 9 den Auftraggeber unverzüglich zu informieren, wenn eine Aufsichtsbehörde beim Auftragnehmer Maßnahmen ergreift, die Daten des Auftraggebers betreffen können, oder wenn Dritte – etwa Strafverfolgungsbehörden – Zugriff auf diese Daten verlangen. Der Auftragnehmer wird einem solchen Verlangen nur nachkommen, soweit er gesetzlich dazu verpflichtet ist, und den Auftraggeber – soweit rechtlich zulässig – vorab unterrichten;
- 10 auf Verlangen des Auftraggebers eine Kontaktperson für Datenschutzfragen zu benennen. Ein Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die Voraussetzungen des Art. 37 DSGVO in Verbindung mit § 38 BDSG nicht vorliegen. Ansprechpartner in Datenschutzfragen ist die Geschäftsführung unter mail@bmpgmbh.de.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die zur Sicherstellung eines dem Risiko angemessenen Schutzniveaus erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in **Anlage 2** beschrieben.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer ist berechtigt, sie anzupassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Anforderung mitzuteilen.

(3) Der Auftraggeber hat sich vor Beginn der Verarbeitung von der Angemessenheit der Maßnahmen überzeugt; mit Abschluss dieses Vertrages bestätigt er dies.

(4) Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen regelmäßig.

§ 6 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt und werden hiermit ausdrücklich genehmigt.

(2) Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, informiert er den Auftraggeber hierüber in Textform mit einer Frist von mindestens vier Wochen vor Beginn der Verarbeitung. Der Auftraggeber kann der Änderung innerhalb von zwei Wochen nach Zugang der Information aus wichtigem, datenschutzrechtlich begründetem Anlass widersprechen.

(3) Widerspricht der Auftraggeber und kann der Auftragnehmer die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht zu wirtschaftlich zumutbaren Bedingungen erbringen, steht beiden Parteien ein Sonderkündigungsrecht hinsichtlich der betroffenen Leistung zu.

(4) Der Auftragnehmer verpflichtet den Unterauftragsverarbeiter vertraglich auf Pflichten, die den Pflichten aus diesem Vertrag entsprechen (Art. 28 Abs. 4 DSGVO). Er wählt ihn sorgfältig aus und überzeugt sich vor Beauftragung sowie danach regelmäßig davon, dass dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat.

(5) Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Einhaltung wie für eigenes Handeln.

(6) Keine Unterauftragsverarbeitung im Sinne dieser Vorschrift sind Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt und die die Verarbeitung der Daten des Auftraggebers nicht zum Gegenstand haben – etwa Telekommunikationsleistungen, Postdienste, Reinigung oder die Entsorgung von Datenträgern. Auch bei solchen Leistungen hat der Auftragnehmer für die Wahrung der Vertraulichkeit zu sorgen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich von der Einhaltung dieses Vertrages und der getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

(2) Der Nachweis erfolgt im Regelfall in Textform. Der Auftragnehmer stellt auf Anforderung den Auszug aus dem Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO, die Beschreibung der technischen und organisatorischen Maßnahmen sowie die Auskunft über die Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung. Ergänzend übermittelt er gegebenenfalls vorhandene Testate und Zertifikate, auch solche seiner Unterauftragsverarbeiter.

(3) **Besteht ein konkreter Anlass** – etwa ein gemeldeter Verstoß gegen den Schutz personenbezogener Daten, begründete Zweifel an der Einhaltung dieses Vertrages oder eine entsprechende Aufforderung einer Aufsichtsbehörde – kann der Auftraggeber eine Überprüfung in den Geschäftsräumen des Auftragnehmers

durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Die Überprüfung ist mit einer Frist von mindestens zwei Wochen anzukündigen, findet während der üblichen Geschäftszeiten statt und darf den Betriebsablauf nicht unangemessen beeinträchtigen.

(4) Der Auftraggeber stellt sicher, dass bei der Kontrolle keine Geschäfts- und Betriebsgeheimnisse des Auftragnehmers und keine Daten anderer Kunden offengelegt werden. Ein vom Auftraggeber beauftragter Prüfer darf kein Wettbewerber des Auftragnehmers sein.

(5) Der Auftragnehmer ist verpflichtet, Auskünfte zu erteilen, soweit dies zur Durchführung einer Kontrolle im Sinne des Art. 28 Abs. 3 lit. h DSGVO erforderlich ist.

§ 8 Verletzung des Schutzes personenbezogener Daten

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens jedoch innerhalb von **48 Stunden** nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten des Auftraggebers (Art. 33 Abs. 2 DSGVO).

(2) Die Mitteilung enthält, soweit dem Auftragnehmer bekannt:

- eine Beschreibung der Art der Verletzung, soweit möglich unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
- die wahrscheinlichen Folgen der Verletzung,
- die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und zur Abmilderung möglicher nachteiliger Auswirkungen,
- den Zeitpunkt der Feststellung sowie einen Ansprechpartner für Rückfragen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei dessen Meldepflicht gegenüber der Aufsichtsbehörde nach Art. 33 DSGVO und bei der Benachrichtigung betroffener Personen nach Art. 34 DSGVO. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen obliegen dem Auftraggeber; der Auftragnehmer nimmt sie nicht eigenständig vor.

(4) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und stimmt sich hierüber mit dem Auftraggeber ab.

(5) Der Auftragnehmer dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich der ergriffenen Abhilfemaßnahmen.

§ 9 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch (Art. 12 bis 23 DSGVO) zu beantworten.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst. Er weist die betroffene Person darauf hin, dass der Auftraggeber Verantwortlicher ist.

(3) Der Auftragnehmer unterstützt den Auftraggeber ferner bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Verletzungen, der Datenschutz-Folgenabschätzung und der vorherigen Konsultation der Aufsichtsbehörde – jeweils unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

(4) Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung der Daten nur nach Weisung des Auftraggebers ein. Von dieser Bindung ausgenommen sind Fälle, in denen eine gesetzliche Verpflichtung des

Auftragnehmers besteht.

§ 10 Vertraulichkeit

(1) Der Auftragnehmer verpflichtet die mit der Verarbeitung befassten Personen vor Aufnahme ihrer Tätigkeit schriftlich zur Vertraulichkeit und unterrichtet sie über die Besonderheiten der Datenverarbeitung im Auftrag sowie über die bestehende Weisungsbindung (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO).

(2) Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit und nach Beendigung dieses Vertrages fort.

(3) Der Auftragnehmer beschränkt den Zugriff auf Daten des Auftraggebers auf diejenigen Personen, die ihn zur Erfüllung ihrer Aufgaben benötigen.

§ 11 Rückgabe und Löschung nach Beendigung

(1) Der Auftraggeber entscheidet nach Art. 28 Abs. 3 lit. g DSGVO, ob die Daten nach Abschluss der Verarbeitung zurückgegeben oder gelöscht werden. Er teilt seine Entscheidung spätestens mit Vertragsende in Textform mit. Trifft er keine Entscheidung, werden die Daten nach Absatz 3 gelöscht.

(2) **Herausgabe in Bereich A:** Verlangt der Auftraggeber die Rückgabe, stellt der Auftragnehmer die gehosteten Datenbestände in einem gängigen, maschinenlesbaren Format bereit. Die Übergabe erfolgt als verschlüsseltes, kennwortgeschütztes Archiv; das Kennwort wird auf getrenntem Weg übermittelt. Der Aufwand wird nach § 12 Abs. 3 vergütet, soweit er über eine einfache Bereitstellung hinausgeht. Diese Regelung entspricht § 17 Abs. 4 der Allgemeinen Geschäftsbedingungen des Auftragnehmers.

(3) **Löschung in Bereich A:** Nach Ablauf eines Monats seit Vertragsende löscht der Auftragnehmer die Datenbestände einschließlich aller Sicherungen. Der Auftraggeber wird vor der Löschung nochmals in Textform hingewiesen. Die Frist gibt ihm Gelegenheit, die Herausgabe zu verlangen oder eine Übernahme durch einen anderen Anbieter zu organisieren.

(4) **Bereiche B und C:** Daten, die der Auftragnehmer zur Bearbeitung eines einzelnen Vorgangs erhalten hat, löscht er **unverzüglich nach Abschluss dieses Vorgangs** einschließlich aller Kopien, Zwischenstände und Sicherungen. Einer gesonderten Aufforderung des Auftraggebers bedarf es nicht. Eine Rückgabe kommt hier regelmäßig nicht in Betracht, weil der Auftragnehmer nur Kopien von Beständen erhält, über die der Auftraggeber selbst verfügt. Ist ein Arbeitsergebnis entstanden, das dem Auftraggeber noch nicht übergeben wurde, stellt der Auftragnehmer es vor der Löschung nach Absatz 2 bereit.

(5) Von der Löschungspflicht ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht besteht. Diese Daten werden gesperrt und nach Ablauf der Aufbewahrungsfrist gelöscht. Der Auftragnehmer teilt dem Auftraggeber auf Anforderung mit, welche Daten hiervon betroffen sind und auf welcher Grundlage sie aufbewahrt werden.

(6) Der Auftragnehmer bestätigt die Löschung dem Auftraggeber auf Anforderung in Textform.

(7) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, darf der Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren.

§ 12 Vergütung

(1) Die Erfüllung der Pflichten aus diesem Vertrag ist mit der Vergütung aus dem Hauptvertrag abgegolten, soweit nachfolgend nichts Abweichendes bestimmt ist.

(2) Die Unterstützung bei einzelnen Anfragen betroffener Personen sowie die Bereitstellung der Nachweise nach § 7 Abs. 2 erfolgen für den Auftraggeber kostenfrei.

(3) Über den üblichen Umfang hinausgehende Mitwirkungsleistungen – insbesondere die Begleitung einer Vor-Ort-Kontrolle nach § 7 Abs. 3, umfangreiche Zuarbeit zu einer Datenschutz-Folgenabschätzung, die Herausgabe umfangreicher Datenbestände nach § 11 Abs. 2 sowie die Wiederherstellung von Daten, deren Verlust nicht vom Auftragnehmer zu vertreten ist – werden nach dem tatsächlichen Aufwand gemäß den jeweils gültigen Stundensätzen des Auftragnehmers vergütet. Der Auftragnehmer weist den Auftraggeber vor Beginn solcher Leistungen auf die Kostenpflicht hin und stimmt den voraussichtlichen Umfang mit ihm ab.

(4) Ergibt eine Kontrolle nach § 7 Abs. 3, dass der Auftragnehmer gegen diesen Vertrag oder datenschutzrechtliche Vorschriften verstoßen hat, trägt er die Kosten der Kontrolle selbst.

§ 13 Haftung

(1) Für die Haftung der Parteien untereinander gelten die Regelungen des Hauptvertrages, soweit nachfolgend nichts Abweichendes bestimmt ist.

(2) Im Außenverhältnis gegenüber betroffenen Personen gilt Art. 82 DSGVO.

(3) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen verantwortlich. Der Auftragnehmer haftet für Schäden nur, soweit er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung beziehungsweise entgegen den rechtmäßig erteilten Weisungen des Auftraggebers gehandelt hat.

§ 14 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages einschließlich seiner Anlagen bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.

(2) **Form des Abschlusses:** Dieser Vertrag wird nach Art. 28 Abs. 9 DSGVO schriftlich geschlossen; das elektronische Format ist ausreichend. Der Abschluss kann daher auch durch Austausch eingescannter oder elektronisch signierter Fassungen erfolgen. Jede Partei erhält eine vollständige Ausfertigung einschließlich der Anlagen.

(3) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrages vor, soweit es um die Verarbeitung personenbezogener Daten im Auftrag geht.

(4) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck am nächsten kommt.

(5) Es gilt das Recht der Bundesrepublik Deutschland.

(6) Ist der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist Gerichtsstand für alle Streitigkeiten aus diesem Vertrag der Sitz des Auftragnehmers. Der Auftragnehmer ist auch berechtigt, am allgemeinen Gerichtsstand des Auftraggebers zu klagen.

(7) Bestandteil dieses Vertrages sind die Anlagen 1 bis 3.

Unterschriften

Auftraggeber	Auftragnehmer
Ort, Datum: _____	Ort, Datum: _____
_____	_____

Auftraggeber	Auftragnehmer
Name, Funktion	bmp GmbH

Anlage 1 – Beschreibung der Verarbeitung

1. Beauftragte Leistungsbereiche

Zutreffendes ist anzukreuzen. Es gelten ausschließlich die angekreuzten Bereiche.

☐ **Bereich A – Webhosting und Betrieb** (Ziffern 2 bis 4)

☐ **Bereich B – Betreuung, Wartung und Fernwartung** (Ziffern 5 bis 6)

☐ **Bereich C – Entwicklung, Datenübernahme und Test mit Echtdateien** (Ziffern 7 bis 8)

Beauftragt der Auftraggeber später eine weitere Leistung, erweitert sich dieser Vertrag entsprechend; der Auftragnehmer stellt ihm die aktualisierte Fassung in Textform zur Verfügung.

Bereich A – Webhosting und Betrieb

2. Gegenstand und Art der Verarbeitung

Der Auftragnehmer stellt Speicherplatz und Rechenleistung bereit und hält die Website oder Anwendung des Auftraggebers zum Abruf über das Internet bereit. Er verarbeitet dabei laufend alle personenbezogenen Daten, die über dieses System erhoben, gespeichert oder übermittelt werden.

Die Verarbeitung umfasst das Speichern, das Bereithalten, das Übermitteln an die abrufenden Endgeräte, das Sichern – soweit vereinbart – und das Löschen.

Der Auftragnehmer nimmt keine inhaltliche Kenntnis der verarbeiteten Daten, soweit dies nicht zur Störungsbeseitigung erforderlich ist und der Auftraggeber ihn hiermit beauftragt hat.

3. Art der personenbezogenen Daten und betroffene Personen

Welche Daten anfallen, bestimmt allein der Auftraggeber durch die Gestaltung seines Angebots. In Betracht kommen insbesondere:

Datenkategorie	Beispiele
Bestandsdaten	Name, Anschrift, Kundennummer
Kontaktdaten	E-Mail-Adresse, Telefonnummer
Zugangsdaten	Benutzernamen, gespeicherte Kennwortprüfwerte
Inhaltsdaten	Eingaben in Formulare, hochgeladene Dateien, Nachrichten
Nutzungsdaten	Zugriffszeitpunkte, aufgerufene Seiten, IP-Adressen in Protokolldateien
Vertrags- und Abrechnungsdaten	Bestellungen, Rechnungen, Zahlungsangaben

Betroffene Personen: Besucher und Nutzer des Angebots des Auftraggebers, dessen Kunden, Interessenten, Mitglieder und Beschäftigte, je nach Ausgestaltung des Angebots.

Der Auftraggeber teilt dem Auftragnehmer vor Beginn der Verarbeitung mit, wenn über sein Angebot besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO verarbeitet werden, etwa Gesundheitsdaten oder Angaben zu religiösen oder gewerkschaftlichen Zugehörigkeiten. Die Parteien stimmen in diesem Fall ab, ob

zusätzliche Schutzmaßnahmen erforderlich sind.

4. Dauer der Verarbeitung in Bereich A

Die Verarbeitung dauert für die Laufzeit des Hostingvertrages an. Nach dessen Ende gilt § 11 Abs. 2 und 3 dieses Vertrages.

Bereich B – Betreuung, Wartung und Fernwartung

5. Gegenstand, Art und Zweck der Verarbeitung

Zugang zu personenbezogenen Daten des Auftraggebers entsteht ausschließlich anlassbezogen, wenn dieser eine Leistung anfordert:

Anlass	Art des Zugangs
Fernwartung	Ansicht und Bedienung eines Systems des Auftraggebers während einer von ihm gestarteten und freigegebenen Sitzung
Fehleranalyse	Übersendung von Protokolldateien, Bildschirmfotos oder Datenausügen durch den Auftraggeber
Pflege und Aktualisierung	Zugriff auf das System des Auftraggebers zur Durchführung vereinbarter Arbeiten

Zweck ist ausschließlich die Erbringung der jeweils angeforderten Leistung. Eine darüber hinausgehende Kenntnisnahme, Auswertung oder Speicherung findet nicht statt.

Eine Fernwartungssitzung kommt nur zustande, wenn der Auftraggeber das Programm startet und die Sitzungsdaten übermittelt. Er sieht während der gesamten Sitzung, welche Handlungen vorgenommen werden, und kann sie jederzeit beenden.

6. Dauer der Verarbeitung in Bereich B

Die Verarbeitung ist auf die Dauer des jeweiligen Vorgangs beschränkt. Nach dessen Abschluss werden die Daten gemäß § 11 Abs. 4 dieses Vertrages gelöscht.

Bereich C – Entwicklung, Datenübernahme und Test mit Echtdaten

7. Gegenstand, Art und Zweck der Verarbeitung

Der Auftraggeber übergibt dem Auftragnehmer produktive Datenbestände, damit dieser sie in ein neues System übernimmt, eine Entwicklung daran erprobt oder einen Fehler nachstellt, der sich nur mit echten Daten reproduzieren lässt.

Die Übergabe erfolgt ausschließlich als verschlüsseltes, kennwortgeschütztes Archiv nach Anlage 2. Der Auftragnehmer legt die Bestände auf einem gesonderten Laufwerk ab, das von der allgemeinen Dateiablage getrennt ist.

Vorrang der Datenminimierung: Vor jeder Übergabe prüfen die Parteien, ob ein anonymisierter, pseudonymisierter oder auf den erforderlichen Ausschnitt reduzierter Bestand genügt. Der Auftragnehmer weist

den Auftraggeber hierauf hin. Nur wenn dies nicht ausreicht, werden Echtdaten übergeben.

8. Dauer der Verarbeitung in Bereich C

Die Verarbeitung ist auf die Dauer des jeweiligen Vorgangs beschränkt. Nach dessen Abschluss werden die Bestände einschließlich aller Kopien gemäß § 11 Abs. 4 dieses Vertrages gelöscht.

9. Weisungsberechtigte und weisungsempfangende Personen

Weisungsberechtigt auf Seiten des Auftraggebers:

Name, Funktion: _____

E-Mail: _____

Telefon: _____

Weitere Person (optional): _____

Der Auftraggeber teilt einen Wechsel der weisungsberechtigten Person unverzüglich in Textform mit. Ein solcher Wechsel ist keine Änderung dieses Vertrages und bedarf keiner neuen Fassung.

Weisungsempfangend auf Seiten des Auftragnehmers:

Die Geschäftsführung der bmp GmbH sowie die von ihr benannten Mitarbeitenden, erreichbar unter mail@bmpgmbh.de und +49 5172 94980-0.

Anlage 2 – Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, die der Auftragnehmer zum Zeitpunkt des Vertragsschlusses getroffen hat. Sie sind Gegenstand seiner Zusage nach § 5 dieses Vertrages.

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

Zutrittskontrolle – Verhinderung des Zutritts Unbefugter zu Datenverarbeitungsanlagen:

- Die Geschäftsräume sind abschließbar und werden außerhalb der Geschäftszeiten verschlossen gehalten.
- Besucher werden nicht unbeaufsichtigt in Räumen mit Datenverarbeitungsanlagen gelassen.
- Die Server für Bereich A stehen in einem Rechenzentrum der Hetzner Online GmbH in Deutschland mit eigener Zutrittssicherung. Der Auftragnehmer hat dort keinen physischen Zutritt.

Zugangskontrolle – Verhinderung der Nutzung von Systemen durch Unbefugte:

- Jede mit der Verarbeitung befasste Person nutzt ein persönliches Benutzerkonto mit eigenem Kennwort; Sammelkonten werden nicht verwendet.
- Für Kennwörter bestehen Vorgaben zu Mindestlänge, Komplexität und Wechsel.
- Arbeitsplätze sperren sich nach einer Zeit ohne Eingabe automatisch.
- Firewall und Virenschutz sind im Einsatz; Betriebssysteme und Anwendungen werden durch regelmäßige Sicherheitsupdates aktuell gehalten.
- Zugriffe von außerhalb des Firmennetzes erfolgen über einen gesicherten VPN-Zugang.
- Für Zugriffe von außen ist eine Zwei-Faktor-Authentifizierung eingerichtet.
- Die administrativen Zugänge zu den Systemen in Bereich A sind auf die damit betrauten Personen beschränkt.

Zugriffskontrolle – Beschränkung des Zugriffs auf das Erforderliche:

- Eingesandte Kundendatenbestände werden ausschließlich auf einem hierfür bestimmten, gesonderten Laufwerk abgelegt, das von der allgemeinen Dateiablage des Auftragnehmers getrennt ist.
- Der Zugriff auf dieses Laufwerk ist technisch auf die mit dem jeweiligen Vorgang befassten Mitarbeitenden beschränkt.

Trennungskontrolle:

- Datenbestände unterschiedlicher Auftraggeber werden getrennt voneinander abgelegt und bearbeitet.
- Jedes gehostete Angebot verfügt über eine eigene Datenbank und einen eigenen Systembenutzer.
- Test- und Entwicklungsumgebungen werden von produktiven Kundendatenbeständen getrennt gehalten.

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO):

- Datenbestände werden ausschließlich als verschlüsseltes, kennwortgeschütztes Archiv nach dem Stand der Technik (AES-256) übergeben. Das Kennwort wird auf einem vom Archiv getrennten Weg übermittelt, in der Regel telefonisch.
- Gehostete Angebote werden ausschließlich über HTTPS ausgeliefert; die verschlüsselte Verbindung wird durch HTTP Strict Transport Security erzwungen.
- Fernwartungsverbindungen sind durch das eingesetzte Produkt Ende-zu-Ende verschlüsselt.
- Der Auftraggeber wird darauf hingewiesen, wenn ein anonymisierter oder reduzierter Datenbestand zur Fehleranalyse ausreicht.

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

Weitergabekontrolle:

- Kundendatenbestände werden nicht an Dritte weitergegeben, außer an die in Anlage 3 genannten Unterauftragsverarbeiter.
- Datenbestände werden nur nach vorheriger Absprache mit dem Auftraggeber angefordert.

Eingabekontrolle:

- Die Bearbeitung von Vorgängen wird im Ticketsystem des Auftragnehmers nachvollziehbar dokumentiert. Dazu gehören auch Änderungen, die an einem Datenbestand des Auftraggebers vorgenommen werden.
- Änderungen am Programmstand gehosteter Angebote werden versioniert und sind nachvollziehbar.
- Fernwartungssitzungen werden nur nach aktiver Freigabe durch den Auftraggeber aufgebaut; dieser sieht durchgehend, welche Handlungen vorgenommen werden.

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

- Die Systeme in Bereich A werden bei der Hetzner Online GmbH in Deutschland betrieben (siehe Anlage 3). Das Rechenzentrum verfügt über eine unterbrechungsfreie Stromversorgung, Netzersatzanlagen und Brandfrüherkennung.
- Die Verarbeitung in den Bereichen B und C erfolgt auf Systemen in den Räumen des Auftragnehmers in Deutschland.
- Die Systeme des Auftragnehmers werden regelmäßig gesichert. Die Wiederherstellbarkeit der Sicherungen wird überprüft.
- Für die Wiederherstellung nach einem Ausfall besteht ein dokumentiertes Vorgehen.

Zur Sicherung der gehosteten Daten: Der Auftragnehmer erstellt Sicherungen der Datenbestände des Auftraggebers in Bereich A nur, soweit dies ausdrücklich vereinbart ist. Ist nichts vereinbart, obliegt die Datensicherung dem Auftraggeber. In den Bereichen B und C erstellt der Auftragnehmer keine Sicherungen.

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

- Alle mit der Verarbeitung befassten Personen sind schriftlich zur Vertraulichkeit verpflichtet.
- Die Mitarbeitenden werden mindestens jährlich zum Datenschutz unterwiesen.
- Für den Umgang mit Verletzungen des Schutzes personenbezogener Daten besteht ein dokumentiertes Vorgehen, das die Einhaltung der Frist nach Art. 33 DSGVO sicherstellt.
- Eingesandte Datenbestände werden nach Abschluss des Vorgangs gelöscht.
- Ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO liegt vor und wird gepflegt; der den Auftraggeber betreffende Auszug wird auf Anforderung zur Verfügung gestellt.
- Die in dieser Anlage beschriebenen Maßnahmen werden mindestens jährlich überprüft und bei Bedarf angepasst.

5. Auftragskontrolle

- Verarbeitung ausschließlich nach Weisung des Auftraggebers, geregelt in diesem Vertrag.
- Sorgfältige Auswahl und vertragliche Bindung von Unterauftragsverarbeitern.

- Benennung fester Ansprechpartner für den Auftraggeber.

Stand dieser Anlage: 19. August 2026. Bei jeder wesentlichen Änderung fortzuschreiben.

Anlage 3 – Unterauftragsverarbeiter

Der Auftraggeber genehmigt den Einsatz der folgenden Unterauftragsverarbeiter:

Unternehmen	Anschrift	Leistung	Bereich	Ort der Verarbeitung
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Bereitstellung und Betrieb der Serverinfrastruktur	A	Deutschland
TeamViewer SE	Bahnhofplatz 2, 73033 Göppingen, Deutschland	Bereitstellung der Fernwartungsverbindung	B	Deutschland / EU
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Betrieb des E-Mail-Systems für die Kommunikation mit dem Auftraggeber	A, B, C	Europäische Union (EU-Datengrenze)

Zu Microsoft: Es gilt das Microsoft Data Protection Addendum einschließlich der Standardvertragsklauseln. Kundendaten werden nach der EU-Datengrenze innerhalb der Europäischen Union gespeichert und verarbeitet. Zu möglichen Zugriffen aus den Vereinigten Staaten siehe § 1 Abs. 6 dieses Vertrages.

Weitere Unterauftragsverarbeiter werden nicht eingesetzt. Insbesondere werden keine Cloud-Dienste zur Speicherung von Datenbeständen des Auftraggebers außerhalb der genannten Infrastruktur und keine externen IT-Dienstleister mit Zugriffsmöglichkeit auf Kundendaten eingesetzt.

Änderungen richten sich nach § 6 dieses Vertrages.

Stand: 19. August 2026