Vertrag zur Auftragsverarbeitung

nach Artikel 28 der Datenschutz-Grundverordnung auf Grundlage der Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/915)

zwischen dem Verantwortlichen
[Name des Unternehmens]
[Straße und Hausnummer]
[PLZ] [Ort], [Land]

und dem Auftragsverarbeiter
Johannes Herbstritt · Herbstritt Webdesign
Schlehenweg 5
71272 Renningen, Deutschland

Muster zur Ansicht – nicht abgeschlossen
Abgeschlossen wird der Vertrag online unter herbstritt.website/services/avv/. Danach erhalten beide Parteien diesen Vertrag mit den Angaben des Verantwortlichen, Vertragsnummer und Prüfsumme als PDF per E-Mail.

Inhalt

Teil A	Ergänzende Vereinbarungen (Geltungsbereich, Laufzeit, Weisungen, Berufsgeheimnisse, Dienste für einzelne Projekte, Vertragsschluss)
Teil B	Standardvertragsklauseln der Europäischen Kommission, Klauseln 1 bis 10
Anhang I	Liste der Parteien
Anhang II	Beschreibung der Verarbeitung je Leistung
Anhang III	Technische und organisatorische Maßnahmen
Anhang IV	Liste der Unterauftragsverarbeiter

MUSTER

Teil A · Ergänzende Vereinbarungen

Der Auftragsverarbeiter betreut für den Verantwortlichen Websites, Onlineshops, Webanwendungen, E-Mail-Postfächer und damit verbundene Dienste. Dabei verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen. Die Parteien regeln dies mit den Standardvertragsklauseln der Europäischen Kommission (Teil B) und deren Anhängen I bis IV. Nach Klausel 2 Buchstabe b ergänzen sie die Klauseln um die folgenden Vereinbarungen. Im Falle eines Widerspruchs haben die Klauseln Vorrang (Klausel 4).

§ 1 Geltungsbereich

(1) Dieser Vertrag gilt für alle Leistungen, mit denen der Verantwortliche den Auftragsverarbeiter beauftragt hat oder künftig beauftragt, zum Beispiel durch Angebot, Auftrag oder Sorglos-Paket (im Folgenden „Hauptvertrag"), soweit dabei personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet werden.
(2) Anhang II beschreibt die Verarbeitung für jede Leistung. Maßgeblich sind die Leistungen, die der Verantwortliche jeweils tatsächlich in Anspruch nimmt.
(3) Dieser Vertrag ersetzt frühere Vereinbarungen der Parteien über die Auftragsverarbeitung für diese Leistungen.

§ 2 Laufzeit

(1) Der Vertrag beginnt mit seinem Abschluss und gilt, solange der Auftragsverarbeiter Leistungen nach § 1 erbringt. Er endet mit der letzten dieser Leistungen, ohne dass es einer Kündigung bedarf. Klausel 10 bleibt unberührt.
(2) Nach dem Ende einer Leistung verfährt der Auftragsverarbeiter mit den Daten nach Klausel 10 Buchstabe d. Für Sicherungskopien gilt Anhang II unter „Dauer der Verarbeitung".

§ 3 Weisungen

(1) Der Hauptvertrag und Anhang II bilden die ersten dokumentierten Weisungen des Verantwortlichen.
(2) Weitere Weisungen erteilt der Verantwortliche in Textform, zum Beispiel per E-Mail. Mündliche Weisungen bestätigt er unverzüglich in Textform.
(3) Weisungsberechtigt sind die gesetzlichen Vertreter des Verantwortlichen und die in Anhang I genannte Kontaktperson. Weisungen nimmt Johannes Herbstritt entgegen.

§ 4 Berufsgeheimnisse

(1) Unterliegt der Verantwortliche einer beruflichen Schweigepflicht, etwa nach § 203 des Strafgesetzbuchs (StGB) als Rechtsanwalt, Steuerberater, Arzt oder Pflegedienst, verpflichtet sich der Auftragsverarbeiter, fremde Geheimnisse, die ihm bei seiner Tätigkeit bekannt werden, geheim zu halten. Er verschafft sich von ihnen nur insoweit Kenntnis, wie es für die Leistung erforderlich ist.
(2) Der Auftragsverarbeiter ist darüber belehrt, dass er sich nach § 203 Absatz 4 StGB strafbar machen kann, wenn er ein fremdes Geheimnis unbefugt offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit bekannt geworden ist.
(3) Weitere Personen darf der Auftragsverarbeiter nur als Unterauftragsverarbeiter nach Klausel 7.7 heranziehen. Er verpflichtet sie in Textform zur Verschwiegenheit und belehrt sie über die Strafbarkeit.

§ 5 Dienste für einzelne Projekte

(1) Dienste, die nur für einzelne Projekte des Verantwortlichen genutzt werden (zum Beispiel KI-Anbieter oder externe Datenbanken), schließt in der Regel der Verantwortliche selbst ab. Der Anbieter ist dann Auftragsverarbeiter des Verantwortlichen und nicht Unterauftragsverarbeiter nach diesem Vertrag. Richtet der Auftragsverarbeiter solche Dienste im Auftrag des Verantwortlichen ein, betreibt oder wartet er sie, gilt dafür dieser Vertrag.
(2) Setzt der Auftragsverarbeiter einen solchen Dienst ausnahmsweise selbst als Unterauftragsverarbeiter ein, vereinbaren die Parteien das vorher in Textform, zum Beispiel im Angebot oder per E-Mail. Die Vereinbarung nennt Name und Anschrift des Anbieters, die Leistung, die Datenarten, den Ort der Verarbeitung und die Garantien für Übermittlungen in Drittländer (Klausel 7.8). Sie ergänzt Anhang IV für diesen Verantwortlichen.

§ 6 Vertragsschluss und Form

(1) Der Vertrag wird in elektronischem Format geschlossen (Artikel 28 Absatz 9 der Verordnung (EU) 2016/679). Der Auftragsverarbeiter bietet ihn unter herbstritt.website/services/avv/ an. Der Verantwortliche nimmt das Angebot an, indem die in Anhang I genannte Kontaktperson das Formular mit den Angaben des Verantwortlichen absendet und dabei bestätigt, zu seiner Vertretung berechtigt zu sein. Einer Unterschrift bedarf es nicht.

MUSTER

(2) Beide Parteien erhalten den Vertrag unmittelbar nach dem Abschluss als PDF-Datei per E-Mail. Vertragsnummer, Zeitpunkt des Abschlusses und Prüfsumme (SHA-256) auf der ersten Seite belegen den Inhalt.
(3) Änderungen und Ergänzungen bedürfen der Textform. Die Liste in Anhang IV ändert sich nach Klausel 7.7 Buchstabe a.
(4) Es gilt das Recht der Bundesrepublik Deutschland. Ist eine Bestimmung unwirksam, bleiben die übrigen wirksam.

MUSTER

Teil B · Standardvertragsklauseln

ABSCHNITT I

Klausel 1 · Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der 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 (Datenschutz-Grundverordnung) sichergestellt werden.
b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
d) Die Anhänge I bis IV sind Bestandteil der Klauseln.
e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2 · Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 · Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 · Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ · Kopplungsklausel

Hinweis: Die Parteien vereinbaren die fakultative Kopplungsklausel nicht. Weitere Parteien können diesem Vertrag nicht beitreten.

ABSCHNITT II · PFLICHTEN DER PARTEIEN

Klausel 6 · Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 · Pflichten der Parteien

7.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines

MUSTER

wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese

Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 · Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

   1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

   2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 · Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

   Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;
c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III · SCHLUSSBESTIMMUNGEN

Klausel 10 · Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

MUSTER

Anhang I · Liste der Parteien

Verantwortlicher

Name	[Name des Unternehmens]
Anschrift	[Straße und Hausnummer] [PLZ] [Ort] [Land]
Kontaktperson	[Name], [Funktion] [E-Mail]
Datenschutzbeauftragter	nicht angegeben
Unterschrift und Beitrittsdatum	Elektronisch abgeschlossen am [Datum] um [Uhrzeit] durch [Name] (Teil A § 6)

Auftragsverarbeiter

Name	Johannes Herbstritt, Herbstritt Webdesign
Anschrift	Schlehenweg 5 71272 Renningen Deutschland
Kontaktperson	Johannes Herbstritt, Inhaber kontakt@herbstritt.website · 0174 3228478
Datenschutzbeauftragter	nicht benannt (keine Pflicht nach Artikel 37 der Verordnung (EU) 2016/679 und § 38 BDSG)
Unterschrift und Beitrittsdatum	Elektronisch abgeschlossen am [Datum] um [Uhrzeit] durch Bereitstellung des Vertrags (Teil A § 6)

MUSTER

Anhang II · Beschreibung der Verarbeitung

Dieser Vertrag gilt für alle Leistungen des Auftragsverarbeiters, soweit der Verantwortliche sie nutzt (Teil A § 1). Für jede Leistung sind Art und Zweck der Verarbeitung, die Kategorien personenbezogener Daten und die Kategorien betroffener Personen beschrieben.

1. Hosting von Websites und Onlineshops

Art der Verarbeitung	Speicherung und Bereitstellung der Website bzw. des Onlineshops auf Servern des Auftragsverarbeiters, einschließlich Datenbanken, Server-Protokollen, Sicherung und Wiederherstellung.
Zweck	Betrieb der Website bzw. des Onlineshops des Verantwortlichen im Internet.
Kategorien personenbezogener Daten	Server-Protokolle (IP-Adresse, Zeitpunkt, aufgerufene Adresse, Browser-Kennung); Inhalte der Website; Benutzerkonten (z. B. Name, E-Mail-Adresse, Passwort-Hash); bei Onlineshops Kunden-, Bestell- und Versanddaten. Vollständige Zahlungsdaten (z. B. Kartennummern) verarbeiten die Zahlungsanbieter des Verantwortlichen, nicht der Auftragsverarbeiter.
Kategorien betroffener Personen	Besucher der Website; Kunden und Interessenten des Verantwortlichen; Nutzer mit Benutzerkonto; Beschäftigte des Verantwortlichen.

2. E-Mail-Postfächer

Art der Verarbeitung	Empfang, Versand und Speicherung von E-Mails, Spam- und Virenprüfung, Sicherung und Wiederherstellung der Postfächer.
Zweck	E-Mail-Kommunikation des Verantwortlichen.
Kategorien personenbezogener Daten	Inhalte, Anhänge und Metadaten von E-Mails (Absender, Empfänger, Zeitpunkt, Betreff); Adressbücher und Kalender, soweit genutzt; Zugangsdaten der Postfächer.
Kategorien betroffener Personen	Beschäftigte des Verantwortlichen; Absender und Empfänger von E-Mails, z. B. Kunden, Lieferanten und Interessenten, sowie in E-Mails genannte Personen.

3. Formular-Dienst

Art der Verarbeitung	Entgegennahme von Eingaben aus Formularen auf der Website des Verantwortlichen, Prüfung auf Vollständigkeit und Missbrauch, Weiterleitung per E-Mail an den Verantwortlichen und gegebenenfalls Eingangsbestätigung an die absendende Person. Die Eingaben werden nicht gespeichert, sondern nur bis zum Versand im Arbeitsspeicher gehalten.
Zweck	Zustellung von Anfragen, Reservierungen und ähnlichen Formulareingaben an den Verantwortlichen.
Kategorien personenbezogener Daten	Formulareingaben (z. B. Name, Kontaktdaten, Nachricht, Termin- oder Reservierungsangaben); für den Missbrauchsschutz kurzzeitig ein mit wechselndem Schlüssel gebildeter Hashwert der IP-Adresse, nur im Arbeitsspeicher.
Kategorien betroffener Personen	Personen, die Formulare auf der Website des Verantwortlichen ausfüllen.

4. Wartung und Pflege

Art der Verarbeitung	Updates, Fehlerbehebung, Sicherung, Wiederherstellung und Änderungen im Auftrag an Websites, Onlineshops und Anwendungen des Verantwortlichen, auch wenn diese bei einem anderen Anbieter betrieben werden. Ein Zugriff auf dort gespeicherte Daten lässt sich dabei nicht ausschließen.
Zweck	Sicherheit, Funktionsfähigkeit und Aktualität der betreuten Systeme.
Kategorien personenbezogener Daten	Alle in den betreuten Systemen gespeicherten Daten, soweit ein Zugriff für die Leistung unvermeidbar ist; im Einzelnen wie beim Hosting.

MUSTER

Kategorien betroffener Personen	Wie beim Hosting.

5. Betrieb von Webanwendungen

Art der Verarbeitung	Bereitstellung und Betrieb von Webanwendungen (z. B. Webapps und Portale) einschließlich Datenbanken, Dateispeicher, Überwachung, Fehlerprotokollen, Sicherung und Wiederherstellung.
Zweck	Betrieb der Anwendung für den Verantwortlichen und deren Nutzer.
Kategorien personenbezogener Daten	Benutzerkonten (z. B. Name, E-Mail-Adresse, Passwort-Hash, Rollen); Inhalte und Nutzungsdaten der Anwendung; Protokoll- und Fehlerdaten.
Kategorien betroffener Personen	Nutzer der Anwendung; Beschäftigte, Kunden und Interessenten des Verantwortlichen.

6. KI-Funktionen und Automationen

Art der Verarbeitung	Automatisierte Verarbeitung von Eingaben (z. B. Anfragen, Texte, Dokumente) durch Automationen und KI-Funktionen, die der Auftragsverarbeiter auf seinen Servern betreibt. Externe KI-Anbieter nur nach Teil A § 5.
Zweck	Die mit dem Verantwortlichen vereinbarten Automationen, z. B. Anfragen vorsortieren oder Antworten als Entwurf vorbereiten.
Kategorien personenbezogener Daten	Die Daten, die der Verantwortliche für die jeweilige Automation vorsieht.
Kategorien betroffener Personen	Je nach Einsatz Kunden, Interessenten und Beschäftigte des Verantwortlichen sowie in den Eingaben genannte Personen.

7. Dateiablage und Dateiaustausch

Art der Verarbeitung	Bereitstellung von Speicherplatz auf Servern des Auftragsverarbeiters zum Ablegen und Austauschen von Dateien.
Zweck	Austausch von Inhalten für Website und Projekte, z. B. Texte, Bilder und Dokumente.
Kategorien personenbezogener Daten	Inhalte der abgelegten Dateien.
Kategorien betroffener Personen	In den Dateien abgebildete oder genannte Personen; Beschäftigte des Verantwortlichen.

Sensible Daten und zusätzliche Garantien

Verarbeitet der Verantwortliche über diese Leistungen sensible Daten im Sinne von Klausel 7.5 (z. B. Gesundheitsdaten in Anfragen an einen Pflegedienst oder Angaben zu Straftaten in Anfragen an eine Kanzlei), sind sie von diesem Vertrag umfasst. Der Auftragsverarbeiter wendet dafür folgende Beschränkungen und Garantien an:

a) Zugriff ausschließlich durch die in Anhang I genannte Kontaktperson des Auftragsverarbeiters;
b) strenge Zweckbindung: keine Auswertung und keine Nutzung für eigene Zwecke;
c) Verschlüsselung bei der Übertragung und in den Sicherungen (Anhang III);
d) keine Weitergabe an Dienste außerhalb von Anhang IV, insbesondere nicht an externe KI-Anbieter, ohne gesonderte Vereinbarung nach Teil A § 5;
e) Verschwiegenheit nach Teil A § 4, soweit der Verantwortliche Berufsgeheimnisträger ist.

Dauer der Verarbeitung

Die Verarbeitung dauert so lange wie die jeweilige Leistung (Teil A § 2). Nach deren Ende löscht der Auftragsverarbeiter die Daten oder gibt sie zurück (Klausel 10 Buchstabe d). Sicherungskopien werden nicht einzeln gelöscht, sondern laufen automatisch ab: bei Websites, Anwendungen und Dateien nach spätestens sechs Monaten, bei E-Mail-Postfächern nach spätestens zwölf Monaten. Bis dahin bleiben sie verschlüsselt und werden nur zur Wiederherstellung verwendet.

MUSTER

Anhang III · Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter ist ein Ein-Personen-Unternehmen. Die folgenden Maßnahmen gelten für alle Leistungen aus Anhang II.

Physische Sicherheit	Alle Server und Sicherungen liegen in Rechenzentren der Hetzner Online GmbH in Deutschland (Nürnberg und Falkenstein), zertifiziert nach ISO/IEC 27001. Zutritt, Videoüberwachung und Brandschutz verantwortet Hetzner. Der Auftragsverarbeiter hat keinen physischen Zugang zu den Servern.
Identifizierung und Autorisierung	Persönliche Zugänge mit Zwei-Faktor-Anmeldung für alle Verwaltungszugänge (Hosting-Konsole, Server-, E-Mail- und Anwendungsverwaltung, Dateiablage). Passwörter sind einzigartig und liegen in einem Passwortmanager. Anmeldung an den Servern per SSH nur mit Schlüssel, Passwort-Anmeldung für den Administrator ist abgeschaltet.
Zugriffskontrolle und Trennung	Verwaltungszugriff auf Server und Daten hat ausschließlich Johannes Herbstritt; es gibt keine Mitarbeiter oder freien Mitarbeiter mit Zugriff. Websites laufen unter getrennten Systembenutzern mit eigenen Datenbanken, Anwendungen in getrennten Containern, E-Mail-Postfächer getrennt nach Domain.
Schutz bei der Übermittlung	Verschlüsselte Verbindungen (TLS/HTTPS) für Websites, Verwaltungsoberflächen und den Formular-Dienst; E-Mail-Übertragung mit TLS, Absenderprüfung über SPF, DKIM und DMARC; Fernzugriff nur per SSH.
Schutz bei der Speicherung	Sicherungen sind verschlüsselt; den Schlüssel besitzt nur der Auftragsverarbeiter. Arbeitsgeräte mit vollständiger Festplattenverschlüsselung und automatischer Bildschirmsperre. Der Formular-Dienst speichert keine Eingaben.
Verfügbarkeit und Wiederherstellung	Nächtliche, inkrementelle Sicherung aller Server auf einen getrennten Sicherungsspeicher (Hetzner Storage Box, Deutschland) mit Ständen für 7 Tage, 4 Wochen und 6 Monate, bei E-Mail 12 Monate. Monatliche Prüfung der Sicherungsarchive. Vor jedem Update ein vollständiges Abbild des Servers, für Web- und Mailserver zusätzlich tägliche Abbilder. Der Ablauf der Wiederherstellung ist dokumentiert.
Systempflege und Konfiguration	Betriebssystem-Updates zweimal im Monat und zeitversetzt je Server, automatische Sicherheitsupdates; Aktualisierung von CMS, Erweiterungen und Paketen im Rahmen der Wartung. Nur benötigte Dienste sind erreichbar.
Protokollierung und Überwachung	Automatische Benachrichtigung über Sicherungen, Updates und Fehler. Protokolle werden nur so lange aufbewahrt, wie es für Betrieb und Sicherheit nötig ist; die Protokolle des Formular-Dienstes enthalten keine Inhalte, E-Mail-Adressen oder IP-Adressen.
Datenminimierung und Löschung	Es werden nur die Daten verarbeitet, die für die Leistung nötig sind. Nach Vertragsende werden Daten gelöscht oder in gängigen Formaten herausgegeben (Dateien und Datenbanken der Website, Postfächer); die Löschung wird auf Wunsch bestätigt. Sicherungen laufen nach Anhang II ab.
Organisation und Überprüfung	Diese Maßnahmen werden mindestens jährlich und bei wesentlichen Änderungen überprüft und angepasst. Unterauftragsverarbeiter werden vor dem Einsatz auf geeignete Garantien geprüft.

Unterstützung des Verantwortlichen (Klauseln 8 und 9)

a) Anträge betroffener Personen leitet der Auftragsverarbeiter unverzüglich an den Verantwortlichen weiter. Auf Weisung gibt er Daten aus den betreuten Systemen heraus, berichtigt oder löscht sie.

b) Verletzungen des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter unverzüglich, möglichst innerhalb von 24 Stunden, nachdem sie ihm bekannt geworden sind, per Telefon und E-Mail an die Kontaktperson aus Anhang I, mit den Angaben aus Klausel 9.2.

c) Für Datenschutz-Folgenabschätzungen und Anfragen der Aufsichtsbehörde stellt er die nötigen Informationen zu seinen Systemen und Maßnahmen bereit.

MUSTER

Anhang IV · Liste der Unterauftragsverarbeiter

Der Verantwortliche genehmigt die Inanspruchnahme folgender Unterauftragsverarbeiter (Klausel 7.7 Buchstabe a, allgemeine schriftliche Genehmigung). Liste Stand 1 vom 19.11.2026.

1. Hetzner Online GmbH

Anschrift	Industriestr. 25, 91710 Gunzenhausen, Deutschland
Kontaktperson	Datenschutzbeauftragter der Hetzner Online GmbH, data-protection@hetzner.com
Beschreibung der Verarbeitung	Bereitstellung der Server (Rechenzentrum, Hardware, Netzwerk) für alle Leistungen aus Anhang II sowie eines getrennten Speichers für die verschlüsselten Sicherungen. Hetzner verarbeitet die Daten nur als Betreiber der Infrastruktur und greift im regulären Betrieb nicht auf Inhalte zu.
Ort der Verarbeitung	Deutschland (Nürnberg und Falkenstein)
Dauer	Für die Dauer dieses Vertrags

Dienste, die nur für einzelne Projekte genutzt werden, sind nicht Teil dieser Liste; für sie gilt Teil A § 5.

MUSTER