Vertrag über Auftragsverarbeitung

im Sinne von Art. 28 Abs. 3 DSGVO

zwischen

___

nachfolgend „Auftraggeber“

und

___

nachfolgend „Auftragnehmer“

1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragnehmer (Art. 28 DSGVO). Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber.

1.2 Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind **Anlage 1** zu entnehmen.

1.3 Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung oder nach vorheriger Weisung des Auftraggebers.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragnehmer zu. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls der Auftragnehmer der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass der Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis – oder bis zu einer Einräumung sonstiger angemessener Sicherheiten durch den Auftraggeber zur Abwendung von Schäden des Auftragnehmers – ausgesetzt werden.

3.2 Eine von den Weisungen oder ohne Weisungen des Auftraggebers abweichende Verarbeitung ist nur zulässig, wenn der Auftragnehmer nach dem Recht der Europäischen Union oder der Mitgliedstaaten zur Datenverarbeitung verpflichtet ist. Im Falle einer solchen Verarbeitung, informiert der Auftragnehmer den Auftraggeber unverzüglich über beabsichtigte oder bereits eingeleitete Verarbeitung, es sei denn, dass das betreffende Recht der Europäischen Union oder des Mitgliedstaates eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet; in diesem Fall erfolgt die Mitteilung unverzüglich, sobald die rechtlichen Hindernisse nicht mehr bestehen.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine Weisung in Textform erfolgen konnte. Der Auftragnehmer hat Person, Datum und Uhrzeit der durch den Auftraggeber erteilten Weisung in angemessener Form zu dokumentieren.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig, im erforderlichen Umfang, zu kontrollieren. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen.

4.2 Die Ergebnisse der Kontrollen und Weisungen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragnehmers

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur zulässig, wenn der Auftragnehmer nach dem Recht der Europäischen Union oder der Mitgliedstaaten zur Datenverarbeitung verpflichtet ist. Im Falle einer solchen Verarbeitung, informiert der Auftragnehmer den Auftraggeber unverzüglich über beabsichtigte oder bereits eingeleitete Verarbeitung, es sei denn, dass das betreffende Recht der Europäischen Union oder des Mitgliedstaates eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet; in diesem Fall erfolgt die Mitteilung unverzüglich, sobald die rechtlichen Hindernisse nicht mehr bestehen.

5.2 Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in **Anlage 2** dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt. Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen regelmäßig und anlassbezogen überprüfen und anpassen.

7. Unterstützungspflichten von Auftragnehmer

Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32-36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Auftragnehmer zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragnehmer ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden

Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in **Anlage 3** aufgeführt. Für die in **Anlage 3** aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

8.2 Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird der Auftragnehmer dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des/der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des/der Subunternehmer(s) als genehmigt. In dringenden Fällen (z.B. bei kurzfristig benötigten Fehleranalysen oder Mängelbeseitigungen), kann der Auftragnehmer die Anzeige- und Widerspruchsfrist für Subunternehmer angemessen verkürzen. Erfolgt ein fristgerechter Widerspruch, dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und/oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.

8.3 Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter (Auftragnehmer) und Unterauftragsverarbeiter (Subunternehmer) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche der Auftragnehmer zur Ausübung von geschäftlichen Tätigkeiten in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen sowie sonstige Maßnahmen, welche die Vertraulichkeit und/oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8.4 Sämtliche Verträge zwischen dem Auftragnehmer und dem Unterauftragsverarbeiter (Subunternehmer) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8.5 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragnehmers

9.1 Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer beim Auftragnehmer angestellten Person, einem Subunternehmer oder einer sonstigen Person, die der Auftragnehmer zur Erfüllung vertraglicher Pflichten eingesetzt hat, begangen wurde.

9.2 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten und das weitere Vorgehen mit ihm abstimmen.

9.3 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von denen auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern für den Auftragnehmer keine rechtliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. Der Auftragnehmer verpflichtet sich, Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist der Sitz des Auftragnehmers Gerichtsstand für alle Streitigkeiten aus diesem Vertrag; ausschließliche Gerichtsstände bleiben hiervon unberührt.

12.3 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.4 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.5 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Ort, Datum	Unterschrift Auftraggeber
Ort, Datum	Unterschrift Auftragnehmer

Anlage 1 - Auftragsdetails

LEISTUNGEN, BEI DENEN DATEN IM AUFTRAG VERARBEITET WERDEN	VERARBEITETE DATENARTEN	BETROFFENE PERSONENKATEGORIEN
Wartung von Webseiten	- IP-Adressen von Webseitenbesuchern - Eingaben in Kontaktformulare - Analysen zum Nutzerverhalten - Kundendaten	- Webseitenbesucher des Auftraggebers - Kunden des Auftraggebers
Webhosting	- IP-Adressen von Webseitenbesucher - Eingaben in Kontaktformulare - Analysen zum Nutzerverhalten - Kundendaten	- Webseitenbesucher des Auftraggebers - Kunden des Auftraggebers

Anlage 2 - Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

1. Sicherung der Arbeitsstätte des Auftragsverarbeiters (Zutrittskontrolle)

Die Arbeitsstätte des Auftragsverarbeiters wird in folgender Weise gegen Einbruch und sonstige unbefugte Zutritte gesichert:

- Manuelles Schließsystem / Türschlösser

2. Sicherung der IT-Systeme des Auftragsverarbeiters (Zugangskontrolle)

Die IT-Systeme des Auftragsverarbeiters werden in folgender Weise gegen unbefugte Zugriffe (z.B. Hackerangriffe) gesichert:

- Passwortvergabe
- Erstellen von Benutzerprofilen in den IT-Systemen
- Zugriffsregeln für Benutzer / Benutzergruppen in den IT-Systemen (Berechtigungskonzept)
- Verwaltung der Berechtigungen durch Systemadministratoren
- Anzahl der Systemadministratoren ist auf das „Notwendigste“ reduziert
- regelmäßige und anlassbezogene Aktualisierung und Überprüfung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)

3. Datenschutz bei den Subunternehmern des Auftragsverarbeiters

Folgende Maßnahmen stellen sicher, dass sich die vom Auftragsverarbeiter ausgewählten Subunternehmer datenschutzkonform verhalten:

- Auswahl der Subunternehmer unter Sorgfaltsgesichtspunkten (insb. hinsichtlich Datensicherheit)
- Abschluss von DSGVO-konformen Auftragsverarbeitungsverträgen mit dem Subunternehmer

4. Sicherung von Daten bei Transport und Übermittlung (Weitergabekontrolle)

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) vor unbefugten Dritten geschützt werden:

- SSL-Verschlüsselung

5. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 - Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(UNTERNEHMENS-) NAME UND ANSCHRIFT	BESCHREIBUNG DER LEISTUNG	LAND DER LEISTUNGSERBRINGUNG
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Hosting & Backup	Deutschland
Strato AG, Otto-Ostrowski-Straße 7, 10249 Berlin	Hosting & Backup	Deutschland