VERTRAG ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG

AUF DER GRUNDLAGE VON STANDARDVERTRAGSKLAUSELN ZWISCHEN VERANTWORTLICHEN UND AUFTRAGSVERARBEITERN GEMÄSS ARTIKEL 28 ABSATZ 7 DER VERORDNUNG (EU) 2016/679

zwischen

dem jeweiligen Vertriebspartner

Straße

PLZ Ort
Land

– im Folgenden „**Verantwortlicher**“ genannt –

und

dem Auftragsverarbeiter

SEPPmail – Deutschland GmbH

Ringstraße 1c

85649 Brunnthal b. München
Deutschland

– im Folgenden „**Auftragsverarbeiter**“ genannt –

- Verantwortlicher und Auftragsverarbeiter gemeinsam im Folgenden:

„die Vertragspartner“ genannt -

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 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

Diese Klausel wurde absichtlich leer gelassen

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 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) 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 zwei Wochen 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.

ANHANG I

BESCHREIBUNG DER VERARBEITUNG

1. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

   Konkretisierend, abweichend oder ergänzend zu den in der Leistungsvereinbarung definierten Kategorien betroffener Personen, kann die Datenverarbeitung prinzipiell sämtliche Personenkategorien umfassen, die der Verantwortliche verarbeitet und im Kontext der vereinbarten Leistung im Zugriffsbereich des Auftragnehmers stehen könnten oder anderweitig verarbeitet werden müssen bzw. könnten. Dies beinhaltet:

   - beschäftigte Personen i.S.d. § 26 BDSG,

   - Endkunden/Kunden,

   - Lieferanten,

   - Sonstige (Partner, andere Dritte, wie Steuerberater etc.).

2. Kategorien personenbezogener Daten, die verarbeitet werden

   Konkretisierend, abweichend oder ergänzend zu den in der Leistungsvereinbarung definierten Arten personenbezogener Daten kann die Datenverarbeitung folgende Arten umfassen:

   - Stammdaten (Name, Adresse, E-Mail, Tel.-Nr., IP-Adresse etc.),

   - Ordnungsdaten (Kunde-Nr., Mitarbeiter-Nr., Mitglieds-Nr. etc.),

   - Telekommunikationsdaten (§ 3 TTDSG),

   - weitere sensible Daten ohne Personenbezug (Geschäftsgeheimnis (§ 2 GeschGehG)).

   Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

   - besondere Arten von personenbezogenen Daten (Art. 9 DSGVO),

   - Finanz-/Mahndaten, Privatgeheimnisse (§ 203 StGB),

   - Sozialdaten gem. § 67 SGB X i.V.m. § 35 SGB I.

3. Art der Verarbeitung

   SEPPmail bietet den Kunden einen zentralisierten, von SEPPmail in deutschen und schweizer Rechenzentren betriebenen Service an. Der seppmail.cloud – Service bietet Signatur, Verschlüsselungs- und E-Mail-Bereinigungsdienste (also die kryptografische Behandlung von E-Mails) für ein- und ausgehende E-Mails von Kunden als zentralen Dienst. Eine Leistungsbeschreibung der einzelnen Services kann dem Dokument «seppmail.cloud-Services – Leistungsbeschreibung» entnommen werden. Das Dokument steht in der jeweils aktuell gültigen Version unter https://www.seppmail.com/de/technologie/cloud/ zum Download bereit.

4. Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

   Zurverfügungstellung von E-Mail Signierungs- sowie Verschlüsselungsmöglichkeiten inkl. Anti-Spam und Anti-Virus durch den Unterauftragnehmer SEPPmail AG.

5. Dauer der Verarbeitung:

   Diese Vereinbarung wird auf unbestimmte Zeit geschlossen und gilt daher unbefristet. Die Dauer der Verarbeitung entspricht jeweils der Dauer der korrespondierenden, vereinbarten Leistungen.

ANHANG II

Technische und organisatorische Maßnahmen,

einschließlich zur Gewährleistung der Sicherheit der Daten

Der Auftragsverarbeiter ist verpflichtet, nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO entweder selbst oder durch die genehmigten Unterauftragnehmer einzuhalten:

1. Maßnahmen zur Pseudonymisierung und Verschlüsselung

Technisch	**Organisatorisch**
Verschlüsselung von Datenträgern auf mobilen, und wo umsetzbar auch auf stationären Systemen	Regelmäßige Schulung der Mitarbeiter im Umgang mit Verschlüsselungstechniken
Verschlüsselte Übertragung und Speicherung von Zugangsdaten	Regelmäßige Kontrolle der Verschlüsselung von Datenträgern und Systemen
Verschlüsselte Datenübertragung über Netzwerke (E-Mail, PGP, HTTPS, VPN)	Regelmäßige Kontrolle und ggf. Aktualisierung der Verschlüsselungsverfahren

2. Maßnahmen zur Sicherstellung der Vertraulichkeit

Technisch	**Organisatorisch**
Aktenvernichtung durch datenschutzkonforme Aktenvernichter	Sorgfältige Auswahl von Reinigungspersonal in den Büroräumen
Datenträgervernichtung durch mechanische Zerstörung und/oder zertifiziertes Entsorgungsunternehmen	Passwörter werden ausschließlich von Benutzern erstellt oder nach der automatischen Erstellung umgehend geändert
Manuelles Schließsystem in den Bürogebäuden	Passwörter werden nach Passwort-Richtlinie erstellt
Sicherheitsschlösser in den Büroräumen	Jeder Systemzugriff wird protokolliert, sofern technisch möglich
Einsatz VPN bei Remote-Zugriffen	Netzwerk und Server sind durch Firewalls geschützt
Anti-Viren-Software Server	Netzwerke sind separiert
Anti-Virus-Software Clients	E-Mails werden nach Möglichkeit verschlüsselt
Firewall	Datenträger werden nach Möglichkeit verschlüsselt

	Datenspeicherung erfolgt grundsätzlich auf geschäftlichen und nicht privaten Endgeräten sowie ausschließlich verschlüsselt
	Fernzugriffe erfolgen ausschließlich über gesicherte Verbindungen (VPN, SSH, TLS)
	Daten für unterschiedliche Zwecke werden – wenn technisch möglich – an getrennten Orten gespeichert
	Alle Mitarbeiter mit Zugriff auf personenbezogene Daten haben sich gesondert zum Datenschutz und zur Verschwiegenheit verpflichtet. Das beinhaltet auch spezielle Geheimnisschutzregelungen wie z.B. die Verpflichtung auf die Einhaltung des Sozialgeheimnisses.
	Mit allen Auftragsverarbeitern wird eine schriftliche Vereinbarung zur Auftragsverarbeitung geschlossen
	Es besteht ein Konzept zur Datenlöschung für alle Systeme
	Es finden regelmäßig Schulungen zum Datenschutz und zur Datensicherheit statt
	Berechtigungskonzept für Zugriff auf Daten
	Richtlinie „Clean Desk“
	Mobile Device Policy
	Regelmäßige Prüfung und Überarbeitung der TOM zur Anpassung an aktuellen Stand der Maßnahmen

3. Maßnahmen zur Sicherstellung der Integrität

Technisch	**Organisatorisch**
Jede Dateneingabe- und Änderung wird technisch protokolliert – sofern technisch möglich	Es gibt ein Rollen- und Berechtigungskonzept zur Eingabe von Daten
Jede Administrationstätigkeit auf EDV-Systemen wird technisch protokolliert, sofern technisch möglich	Alle Mitarbeiter werden regelmäßig geschult, um die Einhaltung der Vorschriften der DSGVO und die Einhaltung der Weisungen sicherzustellen
Zum Validieren von Daten werden Prüfsummen oder ähnliche Methoden eingesetzt, sofern technisch möglich	Arbeitsanweisungen zur Gewährleistung der Datensicherheit und der korrekten Ausführung von Aufträgen werden regelmäßig überwacht

Nutzung von Signaturverfahren, sofern technisch möglich	Datenverarbeitungsprozesse werden regelmäßig durch Tests und/oder Stichprobenkontrollen auf korrekte Funktion überprüft
	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
	Klare Zuständigkeiten für Löschungen
	Regelmäßige Prüfung und Überarbeitung der TOM zur Anpassung an aktuellen Stand der Maßnahmen

4. Maßnahmen zur Sicherstellung der Verfügbarkeit und Wiederherstellung

Technisch	**Organisatorisch**
Regelmäßige systematische Datensicherungen	Zentrale Beschaffung und/oder Freigabe von Hardwarekomponenten mit langer Verfügbarkeit
Regelmäßige Tests der Wiederherstellbarkeit gesicherter Daten (Backups), Redundante Auslegung relevanter technischer Systeme	Zentrale Beschaffung und/oder Freigabe von Software mit langer Verfügbarkeit
Klimatisierung der EDV-Räume	Auswahl von Hardwarelieferanten mit langen Service- und/oder Austauschverträgen
Sicherung der Netzwerkinfrastruktur durch Firewalls	Regelmäßige – wo möglich automatische – Installation von Sicherheitsupdates
Redundante Systeme (Cloud)	IT-Systeme werden durch Fachkräfte betreut, die sich regelmäßig fortbilden
Videoüberwachung Serverraum	Aufbewahrung von Datensicherungen an sicheren, ausgelagerten Orten
	Regelmäßige Prüfung und Überarbeitung der TOM zur Anpassung an aktuellen Stand der Maßnahmen

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Technisch	**Organisatorisch**
Software-Lösungen für Datenschutz-Management im Einsatz	Externer Datenschutzbeauftragter
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener
	Zentrale Dokumenation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ..)

	Dokumentiertes Sicherheitskonzept
	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen
	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

6. Verfahren zur Auftragskontrolle

Organisatorisch
Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
Regelung zum Einsatz weiterer Subunternehmer
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Die von uns verarbeiteten personenbezogenen Daten werden durch die SEPPmail AG in Rechenzentren der **Hetzner Online GmbH**, Gunzenhausen - siehe Anhang IV - gespeichert. Um die Sicherheit der verarbeiteten Daten zu gewährleisten, werden vom Rechenzentrum nach eigenen Angaben die folgenden technischen und organisatorischen Maßnahmen getroffen:

A. Vertraulichkeit

Zutrittskontrolle

- Datacenter-Parks in Nürnberg und Falkenstein
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenter-Park
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
- Verwaltung
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Videoüberwachung an den Ein- und Ausgängen

• Zugangskontrolle

- Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
- Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.

• Datenträgerkontrolle

- Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).

B. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden zur Verfügung gestellt.

C. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

Auftragskontrolle

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
- Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt.

ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Name: SEPPmail AG

Anschrift: Industriestrasse 7, 5432 Neuenhof, Schweiz

Name, Funktion und Kontaktdaten der Kontaktpersonen:
SEPPmail AG: Matthias Leisi, SEPPmail AG, Industriestraße 7, 5432 Neuenhof, Schweiz, +41 56 648 28 38, matthias.leisi@seppmail.ch
Vertreter von nicht in der Union niedergelassenen Verantwortlichen (Art. 27 DSGVO): Timo Schusser, valvisio consulting GmbH, Thorackerstraße 5a, 96052 Bamberg, Deutschland
+49 951/974333-10, timo.schusser@valvisio.de

Beschreibung der Verarbeitung: Technische Zurverfügungstellung des SEPPmail.cloud Dienstes. Eine Leistungsbeschreibung der einzelnen Services kann dem Dokument «seppmail.cloud-Services – Leistungsbeschreibung» entnommen werden. Das Dokument steht in der jeweils aktuell gültigen Version unter https://www.seppmail.com/de/technologie/cloud/ zum Download bereit.

Der Verantwortliche hat die Inanspruchnahme folgender weiterer Unterauftragsverarbeiter durch die SEPPmail AG genehmigt:

1. Name: Hetzner Online GmbH

Anschrift: Industriestr. 25, 91710 Gunzenhausen, Deutschland
Name, Funktion und Kontaktdaten der Kontaktperson: info@hetzner.com, +49 (0)9831 505-0
Beschreibung der Verarbeitung: Zurverfügungstellung von Rechenzentrumsdienstleistungen für die SEPPmail AG

2. Name: SwissSign AG

Anschrift: Sägereistrasse 25, 8152 Glattbrugg, Schweiz
Name, Funktion und Kontaktdaten der Kontaktperson: info@swisssign.com, + 41 848 77 66 55
Beschreibung der Verarbeitung: Ausstellung, Verlängerung, Revozierung und Verwaltung von S/MIME-Zertifikaten

3. Name: SWITCH

Anschrift: Werdstrasse 2, 8021 Zürich, Schweiz
Name, Funktion und Kontaktdaten der Kontaktperson: info@switch.ch, +41 44 268 15 68
Beschreibung der Verarbeitung: Zurverfügungstellung von Cloud-Servern

ANHANG IV

Liste der Parteien

1. Verantwortliche(r):

1.1	**Name und Anschrift**	
1.2	**Name, Funktion und Kontaktdaten der Kontaktperson**	
1.3	**Kontaktdaten des Datenschutzbeauftragten**	

2. Auftragsverarbeiter:

1.4	**Name und Anschrift**	SEPPmail – Deutschland GmbH Ringstraße 1c 85649 Brunnthal b. München Deutschland E-Mail: info@seppmail.de
1.5	**Name, Funktion und Kontaktdaten der Kontaktperson**	Name: Herr Günter Esch Funktion: Geschäftsführer E-Mail-Adresse: esch@seppmail.de Telefon: +49 8104 8999 031
1.6	**Kontaktdaten des/der Datenschutzbeauftragten**	Name: Timo Schusser, valvisio consulting GmbH, Thorackerstraße 5a, 96052 Bamberg, Deutschland Funktion: Externer Datenschutzbeauftragter E-Mail-Adresse: timo.schusser@valvisio.de Telefon: +49 951 / 974 333 – 10

Für den Verantwortlichen

Ort , den

GmbH
Vertreter
Geschäftsführer

Für den Auftragsverarbeiter

Brunnthal, den

SEPPmail – Deutschland GmbH
Günter Esch
Geschäftsführer