Vereinbarung zur Auftragsverarbeitung

Als **Anlage zu den Allgemeinen Nutzungsbedingungen**

- nachfolgend „Leistungsvereinbarung" -

zwischen dem

Kunden

- nachfolgend „Verantwortlicher" –

und der **Sendinblue GmbH**

- nachfolgend „Auftragsverarbeiter" -

- beide nachfolgend gemeinsam „Vertragsparteien" -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Dokumente dieser Vereinbarung:

1. Vereinbarung zur Auftragsverarbeitung
2. Anhänge:
   a) Anhang 1 „Technische und organisatorische Maßnahmen"
   b) Anhang 2 „Unterauftragsverarbeiter"
   c) Anhang 3 „Kontakt und Kommunikation"
   d) Anhang 4 „Prüfbescheinigung"

Die Anhänge 1 - 4 sind Gegenstand dieser Vereinbarung.

Dokumentenhierarchie:

Sollten Bestimmungen dieser Vereinbarung mit denjenigen der Leistungsvereinbarung im Konflikt stehen, geht diese Vereinbarung vor.

Präambel

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

§ 1 Anwendungsbereich und Definitionen

Die Vereinbarung findet Anwendung auf die Verarbeitung aller personenbezogenen Daten, die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden. Allen Begriffen in dieser Vereinbarung, die eine Entsprechung in der DSGVO haben, liegt das jeweilige rechtliche Begriffsverständnis der DSGVO zugrunde. Eine Ausnahme gilt bezüglich des Begriffs „Verantwortlicher". Dieser bedeutet entweder „Verantwortlicher" im Sinne von Art. 4 Nr. 7 DSGVO oder „Auftragsverarbeiter" im Sinne von Art. 4 Nr. 8 DSGVO, je nach Verarbeitungssituation des Kunden.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten bestimmen sich nach der Leistungsvereinbarung und dieser Vereinbarung zur Auftragsverarbeitung. Die allgemeinen Nutzungsbedingungen (https://de.sendinblue.com/legal/termsofuse/) stellen die Leistungsvereinbarung dar und werden bei der Registrierung durch den Verantwortlichen ausdrücklich zugestimmt.

(2) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit der Leistungsvereinbarung. Ist die Leistungsvereinbarung ordentlich kündbar, gelten die Bestimmungen der Leistungsvereinbarung. Im Zweifel gilt eine Kündigung der Leistungsvereinbarung auch als Kündigung dieser Vereinbarung und eine Kündigung dieser Vereinbarung als Kündigung der Leistungsvereinbarung. Der Verantwortliche ist jederzeit zu einer außerordentlichen Kündigung dieser Vereinbarung aus wichtigem Grund berechtigt. Diese hat gem. Anhang 3 „Kontakt und Kommunikation" zu erfolgen. Ein wichtiger Grund liegt insbesondere vor, wenn der Auftragsverarbeiter Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Verantwortlichen nicht ausführen kann oder will. Insbesondere liegt in den Fällen des § 8 Abs. 1 und § 11 Abs. 1 dieser Vereinbarung ein solcher wichtiger Grund vor. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Verantwortliche dem Auftragsverarbeiter zunächst eine angemessene Frist, innerhalb welcher der Auftragsverarbeiter den Verstoß abstellen kann. Nach fruchtlosem Ablauf dieser Frist steht dem Verantwortlichen sodann das Recht zur außerordentlichen Kündigung zu.

(3) Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

Arten von Daten

i. Verantwortlicher und Personen, die vom Verantwortlichen zur Nutzung des Accounts berechtigt sind (zusammenfassend "Nutzer"): Identifikations- und Kontaktdaten (Name, Adresse, Titel, Kontaktdaten, Benutzername, Unternehmens-/Organisationsdaten); Beschäftigungs-/Organisationsdaten (geografischer Standort, Website), Sendeinformationen (E-Mail-Adresse, IP-Adresse, Datum und Uhrzeit).

ii. Kontaktpersonen/Empfängerperson des Verantwortlichen: Identifikations- und Kontaktdaten, wie sie vom Nutzer hochgeladen wurden (Name, E-Mail-Adresse, Telefonnummer, Notizen, importierte Datei); IT-Informationen (IP-Adressen, Öffnungs-/Klickrate, Online-Navigationsdaten).

(4) Folgende Personenkategorien sind durch den Umgang mit den entsprechenden personenbezogenen Daten betroffen:

Personenkategorien

i. Nutzer und

ii. jede Person,

- deren E-Mail-Adresse oder Telefonnummer in der Kundenverteilerliste enthalten ist;
- deren Informationen über die Funktionalitäten der Plattform („Dienste des

Auftragsverarbeiters") gespeichert oder gesammelt werden,
- an die Nutzer E-Mails senden oder mit denen sie auf andere Weise über die Dienste des Auftragsverarbeiters in Kontakt treten oder kommunizieren (zusammenfassend "Abonnenten").

(5) Umfang, Art und Zweck der Datenverarbeitung:

Eine elektronische Verarbeitung von personenbezogenen Daten gem. Absatz 3 findet unter Einsatz der Dienste des Auftragsverarbeiters durch den Verantwortlichen statt. Der Einsatz der Dienste des Auftragsverarbeiters richtet sich nach der Nutzung durch den Verantwortlichen und dieser Auftragsverarbeitungsvereinbarung und stellt dessen grundsätzlich abschließende Weisung an den Auftragsverarbeiter dar. Der Einsatz der Dienste des Auftragsverarbeiters durch den Verantwortlichen führt – je nach Nutzung - zu mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgängen oder Vorgangsreihen im Zusammenhang mit personenbezogenen Daten gem. Absatz 3, die insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung umfassen können.
Die Datenverarbeitung folgt dem der jeweiligen Dienstenutzung durch den Verantwortlichen zugrundeliegenden Zweck, insbesondere zum Management von Geschäftsbeziehungen mit Kontakt- und Empfängerpersonen, zur Kommunikation mit Kontakt- und Empfängerpersonen, zum Direktmarketing sowie zur Transaktionskommunikation mit Kontakt- und Empfängerpersonen.

Um einen sicheren und effizienten Dienst bereitstellen zu können, verarbeitet der Auftragsverarbeiter die personenbezogenen Daten, um Betrug, Phishing, unerwünschte Kommunikation oder jegliches andere unerlaubte Verhalten gegenüber der Plattform, der Infrastruktur oder dem Dienst des Auftragsverarbeiters in Übereinstimmung mit den geltenden Datenschutzgesetzen und -vorschriften und gemäß der Datenschutzrichtlinie des Auftragsverarbeiters zu erkennen, zu überwachen und zu verhindern. Diese Verarbeitung ist für die Bereitstellung des Standard-SaaS-Dienstes des Auftragsverarbeiters erforderlich.

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich und stellt den Auftragsverarbeiter von allen Forderungen oder Ansprüchen Dritter gegenüber dem Auftragsverarbeiter frei, die sich aus einem Verstoß des für die Verarbeitung Verantwortlichen gegen diese Datenverarbeitungsvereinbarung und/oder gegen die geltenden Datenschutzgesetze und -vorschriften ergeben. Der Verantwortliche kann jederzeit den Export, die Berichtigung, die Anpassung und die Löschung der Verarbeitung der personenbezogenen Daten in seinem Account vornehmen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen (unter anderem bei Geltendmachung der Rechte aus Kapitel III sowie im Rahmen der Zusammenarbeit mit Aufsichtsbehörden) unterstützt der Auftragsverarbeiter den Verantwortlichen, soweit der Verantwortliche zur Gewährleistung dieses Schutzes nicht allein in der Lage ist. Insbesondere unterstützt er durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen iSd Art. 32 DSGVO.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter die betroffene Person an den Verantwortlichen verweisen. Der Auftragsverarbeiter wird die betroffene Person dabei unterstützen, den Verantwortlichen zu identifizieren, sofern die betroffene Person hinreichende Informationen hierzu zur Verfügung stellt. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen einer betroffenen Person im Rahmen der Rechte aus Kapitel III vom Verantwortlichen nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

(4) Der Auftragsverarbeiter darf personenbezogenen Daten im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit personenbezogenen Daten gerichtete schriftliche oder elektronische Anordnung des Verantwortlichen (Textform nach 126b BGB). Die Weisungen sind durch die Leistungsvereinbarung, die Dienste des Auftragsverarbeiters und diese Vereinbarung grundsätzlich abschließend festgelegt. Weisungen, die nicht in dieser Aufzählung vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Erteilt der Verantwortliche Einzelweisungen hinsichtlich des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Verantwortlichen zu tragen. Im Falle der Unmöglichkeit oder Unzumutbarkeit, bestimmten Weisungen Folge zu leisten, wird der Auftragsverarbeiter den Verantwortlichen schnellstmöglich informieren. Der Auftragsverarbeiter kann, unbeschadet § 2 Abs. 2, in diesem Fall um Befreiung von der Weisung ersuchen.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße oder könnte gegen datenschutzrechtliche Vorschriften verstoßen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter ist, falls dies unter Berücksichtigung der Schwere des Verstoßes erforderlich ist, berechtigt, den Account auszusetzen oder zu kündigen.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen, soweit die Auskunftserteilung nicht gesetzlich vorgesehen ist, insb. im Fall von § 3 Abs. 4 dieser Vereinbarung. Der Auftragsverarbeiter verwendet die personenbezogenen Daten für die vertraglich vereinbarten Zwecke und ist nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten iSd Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung, soweit der Verantwortliche sich diese nicht selbst beschaffen kann. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(8) Die Verarbeitung der personenbezogenen Daten im Auftrag des Verantwortlichen findet auf dem Gebiet der Europäischen Union sowie in den in Anhang 2 „Unterauftragsverarbeiter" aufgelisteten Drittstaaten statt. Eine Verarbeitung in Drittstaaten ist nur zulässig, wenn sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Einer Verarbeitung von personenbezogenen Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit,

Home-Office, mobiles Arbeiten) wird durch den Verantwortlichen zugestimmt. Der Auftragsverarbeiter gewährleistet die Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO), soweit sie dazu nicht mit den ihnen zur Verfügung stehenden Mitteln jeweils selbst in der Lage sind.

(3) Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n zu benennen, soweit dies gem. Art. 37 DSGVO erforderlich ist. Die Kontaktdaten befinden sich in Anhang 3 „Kontakt und Kommunikation".

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die im Anhang 1 „Technisch-organisatorische Maßnahmen" zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. In Anhang 4 „Prüfbescheinigung" weist der Auftragsverarbeiter die Einhaltung der aufgelisteten technisch-organisatorischen Maßnahmen durch die unabhängige Kontrolle durch den TÜV Rheinland nach.

(2) Technische und organisatorische Maßnahmen unterliegen dem Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der im Anhang 1 „Technisch-organisatorische Maßnahmen" festgelegten Maßnahmen nicht unterschritten werden.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen die Informationen aus § 9 dieser Vereinbarung zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind.

(4) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung, die er für die Prüfung für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung iSd Art. 35 DSGVO) benötigt und unterstützt den Verantwortlichen bei einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO mit den ihm zur Verfügung stehenden Mitteln. Die Zurverfügungstellung von Informationen erfolgt jedoch nur insoweit, als der Verantwortliche diese sich nicht selbst beschaffen kann.

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

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

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

vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

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

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, soweit möglich datenschutzgerecht innerhalb eines Zeitraums von 100 Tagen zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung wird dem Verantwortlichen auf Anforderung bestätigt.

(3) Der Auftragsverarbeiter kann Dokumentationen und Informationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend den jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten personenbezogenen Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2. Der Auftragsverarbeiter bewahrt personenbezogene Daten auch in aggregierter Form für statistische Zwecke auf, sofern diese Daten nicht mehr die Identifizierung der betroffenen Personen ermöglichen und angemessenen Garantien unterliegen, insbesondere im Einklang mit den Art. 5 Abs. 1 lit. b, Art. 14 Abs. 5 lit. b, Art. 17 Abs. 3 lit. d, Art. 21 Abs. 6 und Art. 89 DSGVO.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter erhält die allgemeine Genehmigung jederzeit weitere Auftragsverarbeiter (Subunternehmen) in Anspruch zu nehmen. Die aktuell zur Erfüllung dieses Vertrages hinzugezogenen Subunternehmen sind in Anhang 2 „Unterauftragsverarbeiter" im Einzelnen bezeichnet. Der Auftragsverarbeiter teilt dem Verantwortlichen umgehend jede Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen mit. Der Verantwortliche kann gegen derartige Änderungen Einspruch gem. Art. 28 Abs. 2 S. 2 DSGVO erheben. Der Einspruch ist gem. Anhang 3 „Kontakt und Kommunikation" und innerhalb einer Frist von zwei Wochen ab Mitteilung (§ 187 Abs. 1 BGB) einzulegen. Der Verantwortliche verpflichtet sich, den Einspruch nach Treu und Glauben nur dann einzulegen, wenn schwerwiegende datenschutzrechtliche Bedenken bestehen. Nach wirksamer Einlegung des Einspruchs besteht das Recht des Verantwortlichen, die Auftragsverarbeitung außerordentlich innerhalb von 30 Tagen ab Einspruch zu kündigen. Im Falle eines Einspruchs kann der Auftragsverarbeiter die Auftragsverarbeitung nach eigenem Ermessen ebenfalls kündigen. Die Kündigung hat gem. Anhang 3 „Kontakt und Kommunikation" zu erfolgen.

(2) Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als reine Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt und die sich daher nicht unmittelbar auf die Erbringung der Hauptleistung beziehen. Hierzu gehören – ohne abschließend zu sein – beispielsweise Post-, Transport- und Versanddienstleistungen, Reinigungsdienstleistungen, Bewachungsdienste, Telekommunikationsleistungen, Benutzerservice, Wartung sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit personenbezogener Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem

Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung. Sofern Subunternehmer in Drittländern eingeschalten werden, stellt der Auftragsverarbeiter sicher, dass die zusätzlichen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, jährlich auf Anforderung des Verantwortlichen die erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 5 dieser Vereinbarung dokumentenbasiert zur Verfügung zu stellen, soweit der Verantwortliche sich diese nicht selbst beschaffen kann und sie dem Auftragsverarbeiter vorliegen. Hierfür kann der Verantwortliche Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Dokumentation, Testate von Sachverständigen, Zertifizierung oder interne Prüfungen vorlegen lassen. Der durch diese Kontrolle verursachte Mehraufwand wird mit einem Stundensatz von 75 Euro (Abrechnung im Fünf-Minuten-Takt) angesetzt und ist vom Verantwortlichen zu tragen. Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Sollte eine Aufsichtsbehörde den Auftragsverarbeiter aufgrund schuldhaften Verhaltens des Verantwortlichen kontrollieren, ist der hierfür anfallende Personal- und Materialaufwand vom Verantwortlichen zu tragen.

§ 10 Sonstige Bestimmungen

(1) Sollten die personenbezogenen Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragsverarbeiter wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als Verantwortlichem liegt.

(2) Die Vertragsparteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragsverarbeiter iSd § 273 BGB hinsichtlich der zu verarbeitenden personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen ist.

(3) Der Vertragsparteien sind sich darüber einig, dass jegliche Unterstützungsleistung im Rahmen dieser Vereinbarung durch den Auftragsverarbeiter im vernünftigerweise zu erwartenden Umfang erbracht wird.

§ 11 Schlussbestimmungen

(1) Der Auftragsverarbeiter kann diese Vereinbarung mit einer Vorlaufsfrist von zwei Wochen ändern oder ersetzen. Auf Änderungen oder Ersetzungen der Vereinbarung wird der Verantwortliche per E-Mail oder in seinem Account hingewiesen. Dem Verantwortlichen steht ein außerordentliches Kündigungsrecht zu, welches er innerhalb 30 Tage ab Hinweis ausüben kann. Die außerordentliche Kündigung hat gem. Anhang 3 „Kontakt und Kommunikation" zu erfolgen.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare

Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

(3) Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, Berlin.

Anhang 1 „Technisch-organisatorische Maßnahmen"

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

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

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

§ 3 Konkretisierung der Einzelmaßnahmen
Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:[1]

Nr.	Vertraulichkeit	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	- *Zutritt zu den Büroräumen nur durch oder in Begleitung von berechtigten Personen,* - *Zutrittskontrollsystem zu Büroräumen mithilfe von Schlüsselkonzept (Türsicherung, Eintritt nur mit Schlüssel, dokumentierte Schlüsselvergabe),* - *Lagerung von vertraulichen Dokumenten ausschließlich unter Verschluss in abschließbaren, massiven Schränken.*
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	- *Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren,* - *Kennwortverfahren und Passwortschutz durch verpflichtenden Einsatz eines webbasierten Passwortmanager,* - *Passwortwechsel unter Verwendung von starkem Passwort und 90-Tage-Rhythmus,* - *Zwei-Faktoren-Authentifizierung,* - *Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk,* - *Verpflichtung zur Sperrung der Arbeitsgeräte, MDM Software zur Remote-Sperrung im Einsatz,* - *Einrichtung eines Benutzerstammdatensatz pro User,* - *IP-beschränkter Zugriff auf Server,* - *Berechtigungskonzept für digitale Zugriffsmöglichkeiten.*
3.	**Zugriffskontrolle** Gewährleistung, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und diese bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	- *Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte,* - *Logging,* - *regelmäßige Auswertung der Logfiles,* - *automatisierte 24/7 Überwachung der Logs,* - *Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.*

[1] Klarstellend soll darauf hingewiesen werden, dass nachfolgende Zuordnung der Maßnahmen in die Auflistung aus Art. 32 Abs. 1 lit. a) – d) DSGVO als grobe Kategorisierung zu lesen ist. Einzeln aufgelistete Maßnahmen in der rechten Spalte können hierbei unter mehreren Abschnitten einschlägig sein. Der Übersichtlichkeit halber wurde weitgehend auf eine Mehrfachaufzählung verzichtet.

Nr.	Integrität & Verschlüsselung	Umsetzung der Maßnahme
4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	- *Übertragung und Übermittlung unter 256-Bit-SSL- sowie TLS 1.2 und TLS 1.3 Verschlüsselung,* - *Passwortschutz einzelner Dokumente mit getrennter Kennwortübertragung,* - *VPN-Tunnel,* - *Firewall,* - *Virenschutz,* - *Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO,* - *Nachweis über Versand, Kennzeichnung und Inventarisierung von Datenträgern,* - *sowie bei der nachträglichen Überprüfung: Protokollieren, wer personenbezogenen Daten an dritte Stellen übermittelt und zu welchem Zweck.*
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	- *Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung wird durch Protokollierungssysteme gewährleistet.*
Nr.	**Verfügbarkeit und Belastbarkeit**	**Umsetzung der Maßnahme**
6.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogenen Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	- *tägliches Backup-Verfahren,* - *Spiegeln von Festplatten beim Unterauftragsverarbeiter (RAID-Verfahren),* - *unterbrechungsfreie Stromversorgung beim Unterauftragsverarbeiter (USV),* - *Firewall und Virenschutz bei Auftragsverarbeiter sowie Unterauftragsverarbeiter,* - *Notfallplan,* - *Brandmeldeanlage.*
Nr.	**Vertraulichkeit**	**Umsetzung der Maßnahme**
7.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.	- *Mandantenfähigkeit der Software,* - *Funktionstrennung zwischen Produktion/Test,* - *Entwicklungs- und Testsysteme werden ausschließlich mit Testdaten betrieben.*
8.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	- *Abgrenzung der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter durch eindeutige Vertragsgestaltung mit Abgrenzung der Verantwortlichkeiten zwischen Verantwortlichem und Auftragsverarbeiter,* - *klare Festlegung von Weisungen durch Textformerfordernis,* - *Regelung des Einsatzes von Unterauftragsverarbeitung,* - *Verpflichtung der Beschäftigten auf das Datengeheimnis,* - *Bestellung eines Datenschutzbeauftragten, Schulung der Mitarbeiter bzgl. Einhaltung von Datenschutz und Datensicherheit.*

Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht (Art. 32 Abs. 1 lit. d) DSGVO).

Anhang 2 „Unterauftragsverarbeiter[2]"

§§ 3 und 8 der Vereinbarung zur Auftragsverarbeitung verweisen zur Konkretisierung der Unterauftragnehmer auf diesen Anhang.

Unterauftrags-nehmer	Verhältnis zu Sendinblue GmbH	Sitz Unter-nehmen	Server Standort	An-wendbare Dienst-leistung	Anwendbares Datenschutz-recht/geeignete Garantien Daten-übermittlung Drittländer/ Zertifizierung
Google Cloud France SARL (Google Cloud Platform)[3]	Extern	Frankreich	Deutschland	Hosting	DSGVO, frz./dt. Datenschutzrecht, Zertifizierung ISO 27001
Sendinblue SAS	Mutter-unternehmen	Frankreich	Frankreich	Kundenservice und technische Wartung, Produktdesign	DSGVO, frz. Datenschutzrecht
Silver Line IT Solutions Pvt. Ltd.	Schwester-unternehmen	Indien	Siehe Sendinblue SAS Server	Kundenservice und technische Wartung	Standard-datenschutzklauseln gem. Art. 46 Abs. 2 lit. c) DSGVO und ergänzende Maßnahmen
Sendinblue Inc.	Schwester-unternehmen	USA	Siehe Sendinblue SAS Server	Kunden-service	Standard-datenschutzklauseln gem. Art. 46 Abs. 2 lit. c) DSGVO und ergänzende Maßnahmen
Sendinblue Canada Inc.	Schwester-unternehmen	Kanada	Siehe Sendinblue SAS Server	Kunden-service	Angemessenheits-beschluss gem. Art. 45 DSGVO

[2] Unterauftragsverarbeiter sind die vom Auftragsverarbeiter sorgfältig und unmittelbar ausgesuchten weiteren Auftragsverarbeiter. Für weitere Informationen siehe: https://de.sendinblue.com/wp-content/uploads/sites/3/2022/08/SIB-SAS-List_Subprocessors_for-Germany.pdf.

3 Unmittelbarer Vertragspartner ist unsere Muttergesellschaft.

Anhang 3 „Kontakt und Kommunikation"

§§ 4 und 8 der Vereinbarung zur Auftragsverarbeitung verweisen auf diesen Anhang.

Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters:
Sendinblue GmbH, Datenschutzbeauftragter, Köpenicker Straße 126, 10179 Berlin, support@sendinble.com.

Besondere Kommunikationswege
Der Einspruch gem. § 8 Abs. 1 dieser Vereinbarung ist an den Datenschutzbeauftragten des Auftragsverarbeiters (support@sendinblue.com) zu richten.

Der Auftragsverarbeiter behält sich vor, seinen Informationspflichten, insb. gem. § 8 Abs. 1 und § 11 Abs. 1 dieser Vereinbarung, durch das Einstellen von Mitteilungen im Account des Verantwortlichen nachzukommen.

Die außerordentliche Kündigung seitens des Verantwortlichen aufgrund der § 2 Abs. 2, § 8 Abs. 1 sowie § 11 Abs. 1 dieser Vereinbarung ist an support@sendinblue.com zu richten.

Anhang 4 „Prüfbescheinigung“

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist auf diesen Anhang.

Prüfbescheinigung
Datenschutz

Name und Anschrift des Unternehmens:	Sendinblue GmbH Köpenicker Straße 126 10179 Berlin

Die TÜV Rheinland i-sec GmbH bescheinigt, dass die Sendinblue GmbH folgenden Nachweis erbracht hat:

Die Sendinblue GmbH hat technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten, die sie als Auftragsverarbeiter im Sinne des Art. 28 DSGVO verarbeitet, implementiert.
Die Prüfung basiert auf dem aktuellen Auftragsverarbeitungsvertrag und umfasst insbesondere folgende Aspekte des Schutzes personenbezogener Daten:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit

Der Nachweis der Konformität wurde durch ein Datenschutz-Audit erbracht. Der Prüfbericht Nr. 63013860-01 in der Version 1.0 ist Bestandteil dieser Prüfbescheinigung.

Die Prüfbescheinigung stellt kein akkreditiertes Zertifizierungsverfahren, Siegel oder Prüfzeichen im Sinne der Art. 42, 43 DSGVO dar.

Prüfgrundlage	Der Auftragsverarbeitungsvertrag der Sendinblue GmbH in der Fassung vom Juli 2022 V2.
Berichtsnummer.:	63013860-01
Längstens gültig bis:	28..07.2023

Köln, den 01.08.2022

TÜV Rheinland i-sec GmbH
Am Grauen Stein ·
51105 Köln

i.V. Bernd Zimmer
Datenschutzauditor

TÜVRheinland®
Genau. Richtig.