Vertrag zur Auftragsverarbeitung i.S.d. Art. 28 Datenschutz Grundverordnung (DS-GVO)

zwischen dem Auftraggeber / der Auftraggeberin:

Firmenname:	jotty
Firmenanschrift:	Uhlandstraße, 21
	Bayern - Kitzingen 97318 DE

Im Folgenden auch „Auftraggeber“ genannt, und

der Auftragnehmerin:

Sendinblue GmbH
Köpenicker Str. 126, 10179 Berlin im

Folgenden auch "Sendinblue" genannt.

§1 Gegenstand und Dauer des Auftrags

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

Gegenstand des Auftrags ist die Verwendung von Adressdaten des Auftraggebers zur Versendung von Newslettern per E-Mail und transaktionalen E-Mails.

Die Einzelheiten der Leistungen ergeben sich aus den Allgemeinen Geschäftsbedingungen (https://de.sendinblue.com/legal/termsofuse/), die bei der Registrierung für Sendinblue ausdrücklich vom Auftraggeber akzeptiert werden. Auf diese Leistungen wird hier verwiesen (im Folgenden **Leistungsvereinbarung**)

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Die Regelungen zur Kündigung der Leistungsvereinbarung gelten auch für diesen Vertrag. Eine Beendigung der Leistungsvereinbarung berechtigt beide Parteien zur Kündigung dieses Vertrages

Darüber hinaus sind sich die Parteien darüber einig, dass frühere Verträge zur Auftragsdatenverarbeitung oder Auftragsverarbeitung mit Abschluss dieses Vertrages einvernehmlich beendet werden.

§2 Konkretisierung des Auftragsinhalts (Umfang, Art und Zweck der Datenverarbeitung, Art der Daten, Kreis der Betroffenen)

Umfang, Art und Zweck der Datenverarbeitung beschränken sich auf die Nutzung von Adressdaten zur Versendung von Newslettern per E-Mail.

Gegenstand der Verarbeitung personenbezogener Daten sind Kundendaten vom Auftraggeber.

Die durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen sind Kunden, Geschäftskontakte und Interessenten vom Auftraggeber

Die verarbeiteten Arten von Daten sowie die Kategorien betroffener Personen ergeben sich aus §15 dieses Vertrages.

§3 Technische und organisatorische Maßnahmen, Folgenabschätzung

Der Auftragnehmer ist verpflichtet, die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Erhebung, Verarbeitung, oder Nutzung der personenbezogenen Daten – unter besonderer Berücksichtigung der konkreten Auftragsdurchführung – zu dokumentieren und dem Auftraggeber diese Dokumentation auf Anfrage zur Verfügung zu stellen. Die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen sind zu dem im vorgenannten Zweck in dem als Anlage 1 beigefügten Datensicherheitskonzept aufgeführt und sind Teil dieser Vereinbarung.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung; insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass

diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfte Wirksamkeit wird auf die vorliegende Zertifizierung durch den TÜV Rheinland verwiesen, deren Vorlage dem Auftragnehmer für den Nachweis geeigneter Garantien ausreicht (vgl. Anlage 3).

§4 Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat nur auf Weisung des Auftraggebers die personenbezogenen Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an Sendinblue zwecks Berichtigung, Löschung oder Sperrung seiner Daten wenden sollte, ist der Auftragnehmer verpflichtet, dieses Ersuchen unverzüglich nach Erhalt an den Auftraggeber weiterzuleiten. Etwaige dafür anfallende Kosten trägt der Auftraggeber.

§5 Datenschutzkontrolle und Informationspflicht

Der Auftragnehmer hat nach Art. 28 ff DSGVO folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Auftraggeber auf Anforderung mitgeteilt.
- Wahrung der Vertraulichkeit der Daten entsprechend Art. 29 DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, werden auf die Vertraulichkeit der Daten verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt.
- Unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 57 DSGVO. Dies gilt auch, soweit eine zuständige Behörde nach Art. 83 DSGVO beim Auftragnehmer ermittelt.
- Erstattung von Meldungen an den Auftraggeber in allen Fällen, in denen durch ihn oder die bei ihm beschäftigten Personen oder Unterauftragnehmer Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Dies gilt auch im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten und bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

§6 Unterauftragsverhältnisse

Der Auftragnehmer ist berechtigt, sich für die Erfüllung der Leistungsvereinbarung und/oder dieses Vertrages Unterauftragnehmer zu bedienen. Voraussetzung ist die Zustimmung des Auftraggebers. Die Zustimmung gilt für die zum Zeitpunkt des Vertragsschlusses beauftragten Unterauftragnehmer als erteilt. Die Liste der Unterauftragnehmer ist in Anlage 2 enthalten. Die Zustimmung gilt ferner als erteilt, wenn

- dem Auftraggeber die Identität des Unterauftragnehmers in Textform mitgeteilt wird (Anlage 2)
- die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so gestaltet sind, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen
- bei der Unterbeauftragung dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung eingeräumt werden. Dies umfasst insbesondere das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.
- der Auftraggeber nicht binnen einer Woche ab Mitteilung schriftlich widersprochen hat. Der Auftraggeber darf einen Widerspruch gegen die Einschaltung eines Unterauftragnehmers nur aus wichtigem Grund erheben.

Sendinblue erbringt Ihre Leistungen grundsätzlich aus der Europäischen Union. Aktuell werden von uns die in Anlage 2 näher aufgelisteten Unternehmen der Sendinblue Gruppe zur Erbringung von Support Dienstleistungen eingesetzt. Diese Unterauftragnehmer gewährleisten eine schnelle Bearbeitung von Kundenanfragen und rund-um-die- Uhr erreichbaren Kundensupport. Die entsprechenden Leistungen, wie z.B. deutschsprachiger Support außerhalb der europäischen Tageszeit, werden jedoch äußert selten notwendig. werden jedoch äußert selten notwendig. Daher findet ein Zugriff auf die Daten nur in Ausnahmefällen statt. Sollte dies tatsächlich passieren, so findet die Übertragung auf Grundlage der EU-Standardvertragsklauseln gemäß Art. 46 DSGVO sowie der AV-Verträge nach Art. 28 DSGVO statt. Es findet daher keine grundsätzliche Datenübertragung außerhalb der EU statt, sondern nur dann ein punktueller Zugriff, sofern dies unbedingt erforderlich ist (z.B. Kundensupport bei einem Ticket um 1.00 Uhr nachts).

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§7 Pflichten des Auftraggebers

Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung durch den Auftragnehmer allein verantwortlich und somit „Verantwortlicher“ im Sinne von Art. 4 Nr. 7 DSGVO.

Die Verantwortlichkeit betrifft auch und insbesondere eine etwaige Pflicht zur Führung eines Verzeichnisses nach Art. 30 DSGVO und die Informationspflichten nach Art. 12 - 14 DSGVO.

Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 8 Abs. 9 entsprechend.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§8 Weisungsbefugnis des Auftraggebers/ Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall des Art. 28 Abs. 3 a) DSGVO vor.

Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, welches er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Erteilt der Auftraggeber Einzelweisungen hinsichtlich des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Der Auftragnehmer ist verpflichtet, die zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Offensichtlich datenschutzwidrige Weisungen muss der Auftragnehmer nicht ausführen.

(2) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33-36 DSGVO genannten Pflichten. Für die Erbringung dieser Unterstützungsleistungen berechnen wir eine Vergütung von 75 Euro je angefangener Arbeitsstunde.

(3) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrags fort.

(4) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(5) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(6) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(7) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Für die Erbringung dieser Unterstützungsleistungen berechnen wir eine Vergütung von 75 Euro je angefangener Arbeitsstunde.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Eine Vergütung sowie Schutzmaßnahmen sind hierzu gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart. Für die Erbringung dieser Schutzmaßnahmen berechnen wir eine Vergütung von 75 Euro je angefangener Arbeitsstunde. Die Kosten für die geschäftliche Aufbewahrung von Daten bestimmen sich nach der Größe der Daten sowie der Dauer der Aufbewahrung. Soweit die Aufbewahrung gewünscht ist, ist hierzu eine einzelvertragliche Regelung zu treffen.

(8) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(9) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Für die Erbringung dieser Unterstützungsleistungen berechnen wir eine Vergütung von 75 Euro je angefangener Arbeitsstunde.

§9 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§10 Löschung der personenbezogenen Daten nach Beendigung des zugrundeliegenden Auftrags

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§11 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis

zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen dieses ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion verlangt der Auftragnehmer eine Vergütung in Höhe von 600 Euro pro Arbeitstag verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Die Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§12 Hinweis auf rechtskonformes Verhalten

Der Auftragnehmer weist darauf hin, dass keine Werbung unter Verstoß gegen gesetzliche Vorschriften durch die Auftraggeber versandt werden darf. Die Auftraggeber tragen die Verantwortung für die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung. Dies betrifft auch die Verpflichtung der Auftraggeber nach dem Gesetz gegen unlauteren Wettbewerb (insbesondere nach § 7 UWG). Darüber hinaus weist der Auftragnehmer den Auftraggeber auf dessen Pflicht zur Wahrung des Fernmeldegeheimnisses gemäß Telekommunikationsgesetz (§ 88 TKG).

§13 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei Auftraggeber als “Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser standardisierten Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer separaten, schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Eine Vereinbarung in elektronischem Format (Textform) wird von den Vertragsparteien ebenso als wirksam anerkannt.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht. Anstelle der unwirksamen Teile finde die entsprechende gesetzliche Regelung Anwendung.

(4) Es gilt deutsches Recht.

(5) Gerichtsstand ist Berlin.

§14 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§15 Daten

Die folgenden Arten von personenbezogenen Daten werden im Rahmen dieser Vereinbarung verarbeitet.

Arten von Daten:

Kontaktinformationen (wie E-Mail-Adresse und Telefonnummer);Persönliche Informationen (wie Vor- und Nachname, Geburtsdatum, Geschlecht);

Darüber hinaus sind die folgenden Kategorien natürlicher Personen betroffen:

Kunden und potenzielle Kunden;

Anlage 1: Datensicherheitskonzept

Anlage 2: Benennung Unterauftragnehmer

Anlage 3: Zertifikat TÜV Rheinland

Auftraggeber

Bayern - Kitzingen	20/07/2022
Ort	Datum
Judith Rasp	Frau
Unterschrift	Funktion des Auftraggebers/der Auftraggeberin im Betrieb

Sendinblue GmbH:

Berlin	20/07/2022
Ort	Datum
Dariia Ieremenko	Datenschutzbeauftragte
Unterschrift Sendinblue	Funktion bei Sendinblue

Anlage 1

Datensicherheitskonzept

Maßnahmen zur Datenschutzkontrolle gemäß Art. 32 DS-GVO

Stand 08.04.2020

Bei Fragen zur Sendinblue Informationssicherheit wenden Sie sich bitte an die verantwortliche Stelle

Kontakt

Sendinblue GmbH
Datenschutzbeauftragter
Köpenicker Str. 126
10179 Berlin
Tel.: +49 (0) 30 311 99 510
E-Mail: datenschutz@sendinblue.com

Datenschutzmaßnahmen

Die von Sendinblue getätigten Datenschutzmaßnahmen haben das Ziel der Sicherstellung der Verfügbarkeit der Daten, Integrität, Vertraulichkeit, Nichtverkettbarkeit durch Zweckbestimmung, Tranzparenz durch Prüffähigkeit und Intervenierbarkeit durch Ankerpunkte.

Es werden Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten durchgeführt, welche ein aktuelles Schutzniveau gewährleisten. Ebenso haben unsere Maßnahmen zur Datensicherheit das Ziel einer dauerhaften, hohen Belastbarkeit unserer Systeme und Dienste hinsichtlich der damit verbundenen Datenverarbeitung. Wir stellen die Fähigkeit sicher, die Verfügbarkeit der personenebezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Ferner verwenden wir ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Überdies unternehmen der Verantwortliche sowie der Auftragsverarbeiter Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Die Geschäftsprozesse von Sendinblue orientieren sich an den Vorgaben des Art. 32 der Datenschutz-Grundverordnung (DS-GVO).

§1 Schutz vor unbefugter Kenntniserlangung von Beschäftigten- und Kundendaten sowie anderer schützenswerter personenbezogener Daten

Die im Unternehmen getroffenen Maßnahmen gewährleisten, dass Unbefugte nicht auf solche Datenverarbeitungsanlagen Einfluss nehmen können, auf denen personenbezogene Daten verarbeitet oder gespeichert werden.

Der Auftragnehmer sichert dem Auftraggeber zu, dass Unbefugten durch folgende Maßnahmen der Zutritt sowie der Zugang zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet oder gesichert werden:

- Zutritt zu den Büroräumen nur durch oder in Begleitung von berechtigten Personen
- Zentrale Zutrittsregelung für Büroräume (Schlüsselkonzept)
- Brandmeldeanlage
- Lagerung von vertraulichen Dokumenten ausschließlich unter Verschluss in abschließbaren, massiven Schränken. Der Auftragnehmer sichert darüber hinaus zu, dass Unbefugte durch folgende Maßnahmen an der Benutzung der Datenverarbeitungssysteme gehindert werden:
- Passwortschutz: Passwörter mit min. 8 Zeichen inkl. zwei Sonderzeichen. Passwörter werden alle 90 Tage ändert.
- persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ein Benutzerstammsatz pro User
- IP-beschränkter Zugriff auf Server
- Berechtigungskonzept für digitale Zugriffsmöglichkeiten

Die im Unternehmen getroffenen Maßnahmen der Vertraulichkeit und Integrität gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Darüber hinaus wird sichergestellt, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Geschäftsprozesse von Sendinblue werden durch die nachfolgend aufgeführten Maßnahmen unterstützt:

- differenzierte und aufgabenbezogene Berechtigungen, Profile
- regelmäßige Sichtung von Logfiles
- Verpflichtung aller Mitarbeiter auf das Datenschutzgeheimnis und Telekommunikationsgeheimnis.

Die im Unternehmen getroffenen Maßnahmen gewährleisten eine hinreichende Weitergabekontrolle. Personenbezogene Daten werden bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt, ohne dass überprüft, festgestellt und unterbunden werden kann.

Sendinblue versichert hiermit, dass über die gesetzlich vorgesehenen Ausnahmefälle hinaus keinerlei Daten an Dritte weitergegeben werden. Die zur Erreichung dieses Ziels getroffenen Maßnahmen sind nachfolgend aufgeführt:

- 256-Bit-SSL-Verschlüsselung mit extended validation
- es existieren Regelungen zur Datenvernichtung und Löschung (Löschkonzept) Die im Unternehmen getroffenen Maßnahmen zu Datenintegrität gewährleisten eine hinreichende Eingabekontrolle. Es kann in den Geschäftsprozessen von Sendinblue nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Dies wird durch die nachfolgend aufgeführten Maßnahmen bewirkt:

- Gewährleistung durch Protokollierungs- und Protokollauswertungssystem
- Regelungen der Zugriffsrechte

Die im Unternehmen getroffenen Maßnahmen gewährleisten ebenfalls ein hohes Schutzniveau im Bereich Auftragskontrolle. Die im Auftrag verarbeiteten personenbezogenen Daten werden nur entsprechend der Weisungen des Auftraggebers verarbeitet. Dies wird durch die folgenden Maßnahmen unterstützt:

- schriftlicher Vertrag zur Auftragsverarbeitung gem. Art 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- formalisierte Auftragserteilung

Die im Unternehmen getroffenen Maßnahmen zur Verfügbarkeitskontrolle gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Der Auftragnehmer tätigt die folgenden Maßnahmen:

- Tägliches Backup-Verfahren
- Spiegeln von Festplatten beim Unterauftragnehmer (RAID-Verfahren)
- N o t s t r o m v e r s o r g u n g beim Unterauftragnehmer(USV)
- Virenschutz / Firewall sowohl beim Unterauftragnehmer als auch bei Sendinblue
- Notfallplan
- Brandmeldeanlage

Die im Unternehmen getroffenen Maßnahmen der Trennungskontrolle gewährleisten darüber hinaus, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten ebenfalls getrennt verarbeitet werden können.

Die nachfolgend aufgeführten Maßnahmen sind zur Erreichung dieses Zwecks in die Geschäftsabläufe von Sendinblue implementiert:

- Es ist mandantenfähige Software im Einsatz.
- Entwicklungs- und Testsysteme werden ausschließlich mit Testdaten betrieben

§2 Zertifikat des TÜV-Rheinland

Als weitere Compliance-Maßnahme im Bereich Datenschutz haben wir ein Zertifikat als „Dienstleister mit geprüftem Datenschutz-Management“ vom TÜV-Rheinland erhalten.

Im Rahmen des Datenschutz-Audits erfolgen neben der Nachbereitung der datenschutzrechtlichen Bestandsaufnahme fortlaufende Maßnahmen zur Sicherstellung der datenschutzrechtlichen Vorgaben, welche durch jährliche Tätigkeitsberichte nachgewiesen werden.

Anlage 2

Benennung Unterauftragnehmer

Aktuell werden von uns die in Anlage 2 näher aufgelisteten Unternehmen der Sendinblue Gruppe zur Erbringung von Support Dienstleistungen eingesetzt. Diese Unterauftragnehmer gewährleisten eine schnelle Bearbeitung von Kundenanfragen und rund-um-die-Uhr erreichbaren Kundensupport. Die entsprechenden Leistungen, wie z.B. deutschsprachiges Support außerhalb der europäischen Tageszeit, werden jedoch äußert selten notwendig. Daher findet ein Zugriff auf die Daten nur in Ausnahmefällen statt. Sollte dies tatsächlich passieren, so findet die Übertragung auf Grundlage der EU- Standardvertragsklauseln gemäß Art. 46 DSGVO sowie der AV-Verträge nach Art. 28 DSGVO statt. Es findet daher keine grundsätzliche Datenübertragung außerhalb der EU statt, sondern nur dann ein punktueller Zugriff, sofern dies unbedingt erforderlich ist (z.B. Kundensupport bei einem Ticket um 1.00 Uhr nachts).

Externe Unterauftragnehmer

Hetzner Online GmbH

Industriestr. 25
91710 Gunzenhausen Deutschland

Registergericht Ansbach,
HRB 3204 USt-Id Nr. DE 812871812

Die durch Hetzner erbrachte Teilleistung ist das Hosting der Server an Standorten innerhalb der Bundesrepublik Deutschland.

Unterauftragnehmer der Sendinblue Gruppe

Diese Unterauftragnehmer gewährleisten eine schnelle Bearbeitung von Kundenanfragen und rund-um-die-Uhr erreichbaren Kundensupport. Die entsprechenden Leistungen, wie z.B. deutschsprachiges Support außerhalb der europäischen Tageszeit, werden jedoch äußert selten notwendig. Daher findet ein Zugriff auf die Daten nur in Ausnahmefällen statt. Es findet daher keine grundsätzliche Datenübertragung außerhalb der EU statt, sondern nur dann ein punktueller Zugriff, sofern dies unbedingt erforderlich ist (z.B. Kundensupport bei einem Ticket um 1.00 Uhr nachts).

Sendinblue SAS

55 rue d’Amsterdam, 75008 Paris, Frankreich

Eingetragenim Handels- und Gesellschaftsregister(Registre du Commerce et des Sociétés – RCS) von Pariswith No. 498 019 298

Sendinblue SAS ist das Mutterunternehmen von der Sendinblue GmbH

Sendinblue Inc.

1402 3rd. Ave. Ste. 301, Seattle, WA 98101

tax ID no. 47-3065169

Sendinblue Inc. ist ein Schwesterunternehmen von der Sendinblue GmbH

Sendinblue Canada Enterprise Inc.

240 Richmond St W, Toronto M5V 1V6, ON

Business no. 117472958

Sendinblue Canada Enterprise Inc. ist ein Schwesterunternehmen von der Sendinblue GmbH

Silver Line IT Solutions Pvt. Ltd.

08th Floor, Tower-A, Knowledge Boulevard, Sector 62, Noida 201309 (U.P.) India

Corporate Identification Number U72300DL2007PTC167878

Silver Line IT Solutions Pvt. Ltd. ist ein Schwesterunternehmen von der Sendinblue GmbH

Anlage 3

Prüfung der TOMs durch TÜV Rheinland

TÜVRheinland®
Genau. Richtig.

Bericht

- Vertraulich -

Prüfung der technischen und organisatorischen Maßnahmen

bei der

sendinblue

Sendinblue GmbH

Version 1.0

Bericht Nr. 63013031-01

Köln, den 01. Juli 2021

TÜV Rheinland i-sec GmbH

1 Zusammenfassung

Die TÜV Rheinland i-sec GmbH bestätigt der Sendinblue GmbH die Einhaltung der, den Kunden bereitgestellten, Informationen zu den getroffenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO. Die Prüfung basierte auf den dokumentierten technischen und organisatorischen Maßnahmen der Sendinblue GmbH. Die technischen und organisatorischen Maßnahmen sind Bestandteil des Auftragsverarbeitungsvertrages zwischen der Sendinblue GmbH (Auftragnehmer) und dem jeweiligen Kunden (Auftraggeber). Die aktuelle Version des Auftragsverarbeitungsvertrages sowie der Anlagen, die Gegenstand der Prüfung waren, ist unter https://de.sendinblue.com/wp-content/uploads/sites/3/2021/04/AV_Muster_DE_18.02.2021.pdf verfügbar.

Bei der Prüfung wurden keine Abweichungen festgestellt.