TÜVRheinland®
Genau. Richtig.

Bericht

- Vertraulich -

Prüfung der technischen und organisatorischen Maßnahmen

bei der

Brevo
Sendinblue GmbH

Version 1.0

Bericht Nr. 63016438-01

Köln, den 01. August 2024

TÜV Rheinland i-sec GmbH

Allgemeine Informationen zur durchgeführten Untersuchung

Auftraggeber:	Sendinblue GmbH Köpenicker Straße 126 10179 Berlin
Beauftragtes Institut:	**TÜV Rheinland i-sec GmbH** Am Grauen Stein | 51105 Köln Freigerichter Straße 1-3 | 63571 Gelnhausen Dudweilerstraße 17 | 66111 Saarbrücken Zeppelinstr. 1 | 85399 Hallbergmoos Köln HRB 30644 | USt.-ID-Nr: DE812864532 Tel.: +49 221-806 0 / Fax 0221-806 2295 E-Mail: service@i-sec.tuv.com
Untersuchungsumfang:	Prüfung der technischen und organisatorischen Maßnahmen der Sendinblue GmbH am Standort Berlin.
Mitgeltende Unterlagen:	Auftragsdatenverarbeitungsvertrag inkl. Anlage 1 Datensicherheitskonzept Maßnahmen zur Datenschutzkontrolle gemäß Art. 32 DS-GVO.
Projektleiter:	Bernd Zimmer
Projektmitarbeiter:	-

Inhaltsverzeichnis

1 Zusammenfassung 4
2 Grundlagen und Methodik 5
2.1 Ausgangssituation und Zielsetzung 5
2.2 Geltungsbereich 5
2.3 Prüf-/Audit-Grundlage 5
2.4 Vorgehensweise 5
3 Ergebnis der Prüfung: 5
4 Ergebnisse im Detail 6
5 Allgemeine Hinweise 9

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). Gegenstand der Prüfung waren die „Technisch-organisatorische Maßnahmen“ Stand 30.07.2024 “.

Bei der Prüfung wurden keine Abweichungen festgestellt.

2 Grundlagen und Methodik

Dieser Abschnitt beschreibt Ausgangssituation, Geltungsbereich, Zielsetzung und Prüf- und Bewertungsgrundlagen der durchgeführten Untersuchung.

2.1 Ausgangssituation und Zielsetzung

Das Unternehmen Sendinblue GmbH vertreibt am Markt zwei Produkte: „Newsletter2Go“ und „Brevo“. Während ersteres sich auf den Versand von Newslettern fokussiert, bietet zweiteres ein umfassendes Instrumentarium für KMU bis hin zu Großunternehmen von Marketing- und Sales-Plattform, über Transaktions-Mails bis hin zu Chat-Tools. Diese Dienstleistungen werden als Auftragsverarbeitung im Sinne des Art. 28 DSGVO bereitgestellt. Für die Leistungserbringung werden Auftragsverarbeitungsverträge mit den Kunden abgeschlossen. Die Verträge beinhalten (gemäß Art. 28 Abs. 3 lit. e DSGVO) in Anlage 1 die getroffenen technischen und organisatorischen Maßnahmen, die Gegenstand dieser Prüfung sind.

2.2 Geltungsbereich

Standort der Sendinblue GmbH in Berlin

2.3 Prüf-/Audit-Grundlage

Als Prüfgrundlagen wurden verwendet:

- Technische und organisatorischen Maßnahmen der Firma Sendinblue GmbH.
- EU-Datenschutz-Grundverordnung (EU DS-GVO)

2.4 Vorgehensweise

Im Rahmen einer Ortsbegehung wurden die technischen und organisatorischen Maßnahmen am Standort Berlin nachvollzogen und die Konformität mit den Angaben der Sendinblue GmbH überprüft.

Neben der Ortsbegehung wurden Interviews mit den beteiligten Mitarbeitern durchgeführt und die getroffenen Maßnahmen mit den beschriebenen, respektive mit Kunden vertraglich vereinbarten Maßnahmen, verglichen und bewertet.

Folgende Personen wurden beim Audit befragt:

Betina Russell	ext. Datenschutzbeauftragte

3 Ergebnis der Prüfung:

Die von der Sendinblue GmbH gemachten Angaben im Auftragsverarbeitungsvertrag *„Anhang 1- Technische und organisatorische Maßnahmen“* sind implementiert und entsprechen damit den

vertraglich zugesicherten Maßnahmen. Die Prüfung wurde am 26.07.2024 durchgeführt. Eine aktualisierte Version vom 30.07.2024 wurde im Nachgang zum Audit geprüft und hier dokumentiert.

4 Ergebnisse im Detail

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. Der Auftragsverarbeiter führt ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO.

3. Konkretisierung der Einzelmaßnahmen

Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen[2].

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 und Mitarbeiterlaptops 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,* - *Zugang zu Server via Bastion-Host,* - *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,* - *Logging (Security/User),* - *regelmäßige Auswertung der Logfiles,* - *automatisierte 24/7 Überwachung der Logs,* - *Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.*
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.*
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),* - *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 Entwicklung/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 Vertraulichkeit,* - *Bestellung eines Datenschutzbeauftragten, Schulung der Mitarbeiter bzgl. Einhaltung von Datenschutz und Datensicherheit,* - *Kontrolle der Unterauftragsnehmer.*

[2] 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.

5 Allgemeine Hinweise

Im Hinblick auf den Stichprobencharakter der Untersuchung ist darauf hinzuweisen, dass außerhalb der im Zusammenhang mit dieser Untersuchung abgeprüften Aspekte weitere Stärken, aber auch potentielle Risiken vorhanden sein können.

Obwohl die Durchführung der Prüfung größtmöglicher Sorgfalt unterlag, schließt die TÜV Rheinland i-sec GmbH daher Haftung für vorhandene und nicht erkannte potentielle Risiken aus.

Das Prüfergebnis entbindet das Unternehmen in keiner Weise von der Weiterverfolgung seiner Sicherheitsziele.

Das Unternehmen ist in jedem Fall für seine Maßnahmen zur Sicherstellung seiner Sicherheitsziele selbst verantwortlich.

Jede Haftung für eventuelle Schäden, die aus einer falschen Anwendung der hier gegebenen Informationen resultieren, wird ausgeschlossen.