SENTRICAT

Vertrag zur Auftragsverarbeitung (AVV)

Stand: 28. Oktober 2026 – gilt für alle Tarife mit White-Label-Funktion („Agentur Start“, „Agentur“ und den Agentur-Tarif aus dem Praxishandbuch).

Parteien

zwischen

der Agentur – dem Nutzer von SentriCat mit einem Tarif mit White-Label-Funktion, wie in seinem Konto hinterlegt – – nachfolgend „Verantwortlicher“ –

und

Bodo Mackebrandt, Bahnhofstr. 30, 14712 Rathenow, post@sentricat.de (Betreiber von SentriCat) – nachfolgend „Auftragsverarbeiter“ –

Dieser Vertrag ergänzt die Allgemeinen Geschäftsbedingungen von SentriCat („Hauptvertrag“). Er kommt mit der Buchung eines Tarifs mit White-Label-Funktion zustande; eine Unterschrift ist nicht nötig (Art. 28 Abs. 9 DSGVO). Bei Widersprüchen in Fragen des Datenschutzes geht dieser Vertrag vor.

§ 1 Gegenstand und Dauer

1. Der Auftragsverarbeiter betreibt für den Verantwortlichen die Überwachung von Webseiten mit Kundenverwaltung, Statusseiten, Berichten, Alarm-E-Mails an Kunden und Prüfberichten für Interessenten (White-Label). Dabei verarbeitet er personenbezogene Daten, die der Verantwortliche über seine Kunden und Interessenten eingibt.
2. Daten, die der Auftragsverarbeiter für eigene Zwecke als Verantwortlicher verarbeitet (Konto, Anmeldung, Abrechnung der Agentur selbst), sind nicht Gegenstand dieses Vertrags.
3. Der Vertrag läuft so lange wie der Hauptvertrag und endet mit ihm, jedoch nicht vor Löschung der Daten nach § 7.

§ 2 Art und Zweck der Verarbeitung, Daten, Betroffene

Zweck ist ausschließlich die Erbringung der Leistungen nach dem Hauptvertrag. Die Verarbeitung findet in Deutschland bzw. der EU statt.

Datenart	Beispiele	Betroffene	Verwendung
Kontaktdaten der Kunden	Name, E-Mail-Adresse	Kunden der Agentur und deren Ansprechpartner	Alarm-E-Mails, Monatsberichte
Monitordaten	URLs, Bezeichnungen, erwartete Texte, Weiterleitungsziele	Kunden und Interessenten, soweit Personenbezug besteht (z. B. Einzelunternehmer)	Prüfung der Webseiten
Prüfergebnisse	Status, Antwortzeiten, Fehlercodes, Ausfälle, SSL-Daten, Ausschnitt der Antwort bei Fehlern	wie oben	Dashboard, Statusseiten, Berichte
Statusseiten-Inhalte	Kundenname, Logo, Monitorbezeichnungen	wie oben	öffentliche Statusseite unter seitenstatus.de
Telefonnummern (optional)	Nummern für SMS-Alarme, die die Agentur hinterlegt	Mitarbeiter der Agentur	SMS-Alarme

Besondere Kategorien von Daten (Art. 9 DSGVO) werden nicht verarbeitet und dürfen nicht eingegeben werden.

§ 3 Weisungen

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Die Weisungen ergeben sich aus dem Hauptvertrag und aus den Einstellungen, die der Verantwortliche in SentriCat vornimmt (z. B. welche Kunden welche Mails erhalten). Weitere Weisungen erteilt er in Textform.
2. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies unverzüglich mit und darf die Ausführung bis zur Klärung aussetzen.
3. Eine Verarbeitung ohne Weisung erfolgt nur, wenn das Recht der EU oder Deutschlands dazu verpflichtet; der Auftragsverarbeiter teilt dies vorher mit, soweit das zulässig ist.

§ 4 Pflichten des Auftragsverarbeiters

1. **Vertraulichkeit:** Zugriff auf die Daten hat nur der Betreiber selbst. Setzt er weitere Personen ein, verpflichtet er sie vorher zur Vertraulichkeit.
2. **Sicherheit:** Er trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, beschrieben in Anlage 2. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt.
3. **Betroffenenrechte:** Er unterstützt den Verantwortlichen bei Anfragen von Betroffenen (Auskunft, Berichtigung, Löschung). Die meisten Anfragen kann die Agentur selbst in SentriCat erledigen, etwa durch Bearbeiten oder Löschen eines Kunden. Erreicht eine Anfrage den Auftragsverarbeiter direkt, leitet er sie unverzüglich weiter.
4. **Datenpannen:** Er meldet eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, per E-Mail an die Adresse des Kontos – mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt.
5. **Weitere Unterstützung:** Er unterstützt den Verantwortlichen im zumutbaren Rahmen bei Datenschutz-Folgenabschätzungen und Konsultationen der Aufsichtsbehörde (Art. 35, 36 DSGVO).

§ 5 Unterauftragnehmer

1. Der Verantwortliche genehmigt die in Anlage 1 genannten Unterauftragnehmer.
2. Neue oder ersetzte Unterauftragnehmer kündigt der Auftragsverarbeiter mindestens 30 Tage vorher per E-Mail an. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Findet sich keine Lösung, kann er den Hauptvertrag zum Zeitpunkt des Wechsels kündigen.
3. Der Auftragsverarbeiter verpflichtet jeden Unterauftragnehmer vertraglich auf ein gleichwertiges Datenschutzniveau.
4. Dienste, an die SentriCat Nachrichten nur auf Einstellung der Agentur sendet (Telegram, Slack, eigene Webhooks), sind keine Unterauftragnehmer. Die Agentur wählt sie selbst und ist für deren Einsatz verantwortlich.

§ 6 Kontrollrechte

1. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO nötig sind.
2. Vor-Ort-Kontrollen sind nach Anmeldung mit angemessener Frist (in der Regel 14 Tage) zu üblichen Geschäftszeiten möglich, ohne den Betrieb zu stören. Den Aufwand trägt der Verantwortliche, sofern die Kontrolle keinen Verstoß ergibt.

§ 7 Löschung und Rückgabe

1. Die Agentur kann Kunden, Monitore und Interessenten-Checks jederzeit selbst löschen. Rohdaten der Prüfungen werden automatisch nach 72 Stunden gelöscht; zusammengefasste Statistiken bleiben bis zur Löschung des Monitors.
2. Nach Ende des Hauptvertrags bleiben die Daten zunächst im pausierten Konto, damit die Agentur sie einsehen und exportieren kann. Löscht sie ihr Konto oder verlangt sie die Löschung, löscht der Auftragsverarbeiter alle Daten innerhalb von 30 Tagen.
3. Sicherungskopien werden im regulären Zyklus überschrieben, spätestens nach [30] Tagen.

4. Auf Anfrage bestätigt der Auftragsverarbeiter die Löschung in Textform.

§ 8 Haftung

Die Haftung gegenüber Betroffenen richtet sich nach Art. 82 DSGVO. Im Verhältnis zwischen den Parteien gelten die Haftungsregeln des Hauptvertrags (Ziffer 11 der AGB).

§ 9 Schlussbestimmungen

1. Änderungen dieses Vertrags bedürfen der Textform.
2. Es gilt deutsches Recht. Sollten einzelne Bestimmungen unwirksam sein, bleibt der übrige Vertrag wirksam.
3. Anlagen: 1 – Unterauftragnehmer, 2 – Technische und organisatorische Maßnahmen.

Anlage 1 – Unterauftragnehmer

Unterauftragnehmer	Leistung	Betroffene Daten	Ort der Verarbeitung
Variomedia AG, August-Bebel-Straße 68, 14482 Potsdam	Hosting von Anwendung und Datenbank, E-Mail-Versand (auch Kunden-Alarme über seitenstatus.de)	alle Daten nach § 2	Deutschland
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg	Prüfdienst (AWS Lambda), der die überwachten URLs aufruft	Monitordaten und Prüfergebnisse, keine Kontaktdaten	EU, Region [Frankfurt, eu-central-1]
seven.io, [Firma und Anschrift], Kiel	Versand von SMS-Alarmen	Telefonnummern, Monitorbezeichnung, Status	Deutschland

AWS gehört zu einem US-Konzern. Ein Zugriff aus den USA ist rechtlich nicht ganz auszuschließen. Abgesichert ist das über das AWS Data Processing Addendum mit Standardvertragsklauseln und die Zertifizierung unter dem EU-US Data Privacy Framework.

Nicht in der Liste:

- **Web-Push-Dienste** der Browser-Hersteller (z. B. Google, Apple, Mozilla) leiten Push-Mitteilungen nur an Geräte der Agentur weiter. Die Inhalte sind Ende-zu-Ende verschlüsselt (RFC 8291) und für den Push-Dienst nicht lesbar.
- **Digistore24** wickelt nur die Bezahlung der Agentur selbst ab und erhält keine Daten ihrer Kunden.
- **Telegram, Slack, Webhooks:** siehe § 5 Abs. 4.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Bereich	Maßnahmen
Zutritt (Rechenzentrum)	Server bei Variomedia AG in Deutschland; physischer Schutz nach den technischen und organisatorischen Maßnahmen des Hosters [kurz zusammenfassen]
Zugang zu Systemen	Zugriff auf Server, Datenbank und AWS nur durch den Betreiber, mit persönlichen Zugangsdaten und Zwei-Faktor-Anmeldung, wo der Dienst sie anbietet
Zugriff in der Anwendung	Jede Agentur sieht nur eigene Kunden und Monitore (Prüfung bei jeder Abfrage); Admin-Bereich nur für die Admin-Rolle; Zwei-Faktor-Anmeldung (TOTP) verpflichtend für Admins und Agentur-Tarife; Passwörter als Hash gespeichert, mindestens 8 Zeichen; TOTP-Geheimnisse verschlüsselt; Sitzungen laufen nach 7 Tagen Inaktivität ab; Anmeldeversuche begrenzt
Übertragung	Ausschließlich HTTPS mit HSTS; Schnittstelle zwischen Prüfdienst und Anwendung mit HMAC-SHA256 signiert; Zahlungsbenachrichtigungen mit Signaturprüfung; Web-Push-Inhalte verschlüsselt; Cookies nur über HTTPS
Schutz der Anwendung	CSRF-Schutz für alle Formulare; Sicherheits-Header (u. a. Content-Security-Policy, X-Frame-Options); Schutz gegen Aufruf interner Adressen (SSRF) bei allen vom Nutzer angegebenen URLs; Logo-Uploads nur als Bilddatei, ohne Skriptausführung
Protokollierung	Rohdaten der Prüfungen 72 Stunden; Versand von Benachrichtigungen wird protokolliert; Änderungen im Admin-Bereich werden protokolliert

Bereich	Maßnahmen
Trennung	Daten aller Nutzer in einer Datenbank, logisch getrennt über die Kontozuordnung; Interessenten-Checks sind zusätzlich von allen Kundenlisten getrennt
Verfügbarkeit	[Datensicherung: Intervall, Aufbewahrung, Speicherort]; Überwachung des Prüfdienstes über einen Health-Endpunkt; Wiederherstellung von Sicherungen wird [jährlich] getestet
Auftragskontrolle	Unterauftragnehmer nur nach Anlage 1, jeweils mit eigenem AVV
Überprüfung	Regelmäßige Sicherheitsprüfung des Codes (zuletzt Oktober 2026) und zeitnahes Einspielen von Sicherheitsupdates