

AVV

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

gemäß Artikel 28 Datenschutz-Grundverordnung

Stand: 28. September 2026

zwischen

dem im Rahmen des Kauf- beziehungsweise Registrierungs Vorgangs bezeichneten
Unternehmenskunden

– nachfolgend „Auftraggeber“ –

und

Anna-Lena Meyringer
Einzelunternehmerin, handelnd unter Seitenwacht
c/o Impressumservice Dein-Impressum
Stettiner Str. 41
35410 Hungen
Deutschland

Datenschutzkontakt: datenschutz@seitenwacht.de

– nachfolgend „Auftragnehmer“ –

wird folgende Vereinbarung zur Auftragsverarbeitung geschlossen.

PRÄAMBEL

Der Auftraggeber nutzt die Software Seitenwacht zur automatisierten Überwachung von Websites und digitalen Funktionswegen. Dabei kann Seitenwacht personenbezogene Daten verarbeiten, die der Auftraggeber kontrolliert.

Diese Vereinbarung konkretisiert die Rechte und Pflichten der Parteien nach Artikel 28 DSGVO. Sie ergänzt den Hauptvertrag über die Nutzung der Seitenwacht-Software.

Der Hauptvertrag bestimmt die geschuldete Softwareleistung. Diese Vereinbarung gilt ausschließlich für Verarbeitungen, bei denen der Auftragnehmer personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers verarbeitet.

1. GEGENSTAND UND GELTUNGSBEREICH

1.1 Diese Vereinbarung gilt für alle personenbezogenen Daten, die der Auftragnehmer im Rahmen der Bereitstellung, des Betriebs, der Wartung und des Supports von Seitenwacht im Auftrag des Auftraggebers verarbeitet.

1.2 Gegenstand, Dauer, Art und Zweck der Verarbeitung, Datenarten und Kategorien betroffener Personen ergeben sich aus Anlage 1 und dem Hauptvertrag.

1.3 Diese Vereinbarung geht bei datenschutzrechtlichen Widersprüchen dem Hauptvertrag vor. Im Übrigen bleibt der Hauptvertrag unberührt.

1.4 Verarbeitungen, für die der Auftragnehmer eigene Zwecke und Mittel bestimmt, insbesondere eigene Vertrags-, Abrechnungs-, Sicherheits- und gesetzliche Nachweispflichten, fallen nicht unter diese Auftragsverarbeitung. Für diese Verarbeitungen ist der Auftragnehmer selbst Verantwortlicher.

2. ROLLEN UND VERANTWORTLICHKEIT

2.1 Der Auftraggeber ist Verantwortlicher im Sinne von Artikel 4 Nummer 7 DSGVO. Der Auftragnehmer ist für die von dieser Vereinbarung erfassten Tätigkeiten Auftragsverarbeiter im Sinne von Artikel 4 Nummer 8 DSGVO.

2.2 Der Auftraggeber entscheidet über die Zulässigkeit, die Zwecke und die wesentlichen Mittel der Verarbeitung. Er stellt sicher, dass die Überwachung der eingetragenen Websites, Formulare, Zielpostfächer und sonstigen Prüfziele rechtmäßig ist und erforderliche Informationen, Berechtigungen und Rechtsgrundlagen vorliegen.

2.3 Der Auftraggeber darf nur Websites und Postfächer einbinden, die er selbst betreibt oder zu deren Überwachung und technischer Prüfung er ausdrücklich berechtigt beziehungsweise beauftragt ist.

2.4 Der Auftragnehmer verarbeitet Daten nur zur Erbringung der vereinbarten Seitenwacht-Leistungen und nicht zu eigenen Werbe-, Profilbildungs- oder sonstigen vertragsfremden Zwecken.

3. WEISUNGSGEBUNDENE VERARBEITUNG

3.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers.

3.2 Als dokumentierte Weisungen gelten insbesondere die Konfiguration im Kundenkonto, die Auswahl von Websites, Seiten, Formularen, Buttons, Prüfintervallen und Empfängern sowie Mitteilungen über die vereinbarten Supportkanäle.

3.3 Weisungen, die den Leistungsumfang des Hauptvertrags wesentlich verändern, können eine gesonderte Vereinbarung und eine angemessene Vergütung erfordern. Gesetzliche Pflichten bleiben unberührt.

3.4 Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung aussetzen, bis die Weisung bestätigt, geändert oder zurückgenommen wurde.

3.5 Ist der Auftragnehmer gesetzlich zu einer Verarbeitung verpflichtet, informiert er den Auftraggeber vorab, soweit das anwendbare Recht dies zulässt.

4. PFLICHTEN DES AUFTRAGNEHMERS

4.1 Der Auftragnehmer organisiert seinen Verantwortungsbereich so, dass die Anforderungen der DSGVO und dieser Vereinbarung erfüllt werden.

4.2 Er verarbeitet nur die für den vereinbarten Zweck erforderlichen Daten, beschränkt Zugriffe nach dem Erforderlichkeitsprinzip und schützt die Daten vor unbefugter oder unrechtmäßiger Verarbeitung, Verlust, Zerstörung und Schädigung.

4.3 Er unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Erfüllung der in dieser Vereinbarung genannten Datenschutzpflichten.

4.4 Er führt, soweit gesetzlich erforderlich, ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten nach Artikel 30 Absatz 2 DSGVO und arbeitet mit der zuständigen Aufsichtsbehörde zusammen.

4.5 Der Datenschutzkontakt des Auftragnehmers ist unter datenschutz@seitenwacht.de erreichbar.

5. VERTRAULICHKEIT

5.1 Der Auftragnehmer setzt nur Personen ein, die auf Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.2 Zugriff erhalten ausschließlich Personen, die ihn zur Erfüllung ihrer Aufgaben benötigen. Die Verpflichtung besteht auch nach Ende ihres Einsatzes fort.

5.3 Der Auftragnehmer unterrichtet die eingesetzten Personen über die maßgeblichen Datenschutz- und Sicherheitsvorgaben.

6. SICHERHEIT DER VERARBEITUNG

6.1 Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung angemessene technische und organisatorische Maßnahmen nach Artikel 32 DSGVO.

6.2 Die zum Zeitpunkt des Vertragsschlusses vereinbarten Maßnahmen sind in Anlage 2 beschrieben.

6.3 Der Auftragnehmer darf die Maßnahmen an technische Entwicklungen anpassen, wenn das vereinbarte Schutzniveau nicht unterschritten wird.

6.4 Wesentliche Änderungen, die das Schutzniveau betreffen, werden dokumentiert und dem Auftraggeber auf Anfrage mitgeteilt.

7. UNTERAUFTRAGNEHMER

7.1 Der Auftraggeber erteilt die allgemeine schriftliche Genehmigung, die in Anlage 3 genannten Unterauftragnehmer einzusetzen.

7.2 Der Auftragnehmer informiert den Auftraggeber mindestens 14 Kalendertage vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragnehmers.

7.3 Die Information darf elektronisch erfolgen und muss Name, Leistung, Verarbeitungsort und gegebenenfalls die Grundlage eines Drittlandtransfers enthalten.

7.4 Der Auftraggeber kann innerhalb dieser Frist aus einem sachlich begründeten datenschutzrechtlichen Grund widersprechen. Die Parteien bemühen sich um eine zumutbare Lösung.

7.5 Ist eine Lösung nicht möglich und ist der betreffende Unterauftragnehmer für die Leistung erforderlich, kann jede Partei die betroffene Leistung aus wichtigem Grund beenden.

7.6 Der Auftragnehmer verpflichtet jeden Unterauftragnehmer vertraglich zu Datenschutzpflichten, die den Pflichten dieser Vereinbarung im Wesentlichen entsprechen.

7.7 Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten des Unterauftragnehmers verantwortlich.

7.8 Reine Nebenleistungen ohne Zugriff auf personenbezogene Daten gelten nicht als Unterauftragsverarbeitung. Wartungs- oder Supportleistungen mit möglichem Datenzugriff fallen dagegen unter diese Regelung.

8. UNTERSTÜTZUNG BEI BETROFFENENRECHTEN

8.1 Der Auftragnehmer unterstützt den Auftraggeber durch geeignete technische und organisatorische Maßnahmen bei Anträgen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch, soweit die verarbeiteten Daten und die Art der Leistung dies betreffen.

8.2 Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter.

8.3 Der Auftragnehmer beantwortet eine solche Anfrage nicht selbst, sofern keine dokumentierte Weisung des Auftraggebers oder eine gesetzliche Pflicht besteht.

9. UNTERSTÜTZUNG BEI DATENSCHUTZPFLICHTEN

9.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der verfügbaren Informationen bei:

- der Sicherheit der Verarbeitung,
- der Meldung und Benachrichtigung von Datenschutzverletzungen,
- Datenschutz-Folgenabschätzungen und
- vorherigen Konsultationen nach den Artikeln 32 bis 36 DSGVO.

9.2 Die Unterstützung erfolgt im Rahmen des vereinbarten Leistungsumfangs.

9.3 Außergewöhnlicher Zusatzaufwand kann nach vorheriger Abstimmung angemessen vergütet werden, soweit der Anlass nicht vom Auftragnehmer zu vertreten ist.

10. VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

10.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, soweit Daten des Auftraggebers betroffen sind.

10.2 Die Meldung enthält, soweit verfügbar:

- die Art des Vorfalls,
- die betroffenen Daten und Personengruppen,
- den ungefähren Umfang,
- die wahrscheinlichen Folgen,
- bereits getroffene oder vorgeschlagene Gegenmaßnahmen und
- eine Kontaktstelle für Rückfragen.

10.3 Liegen bei der ersten Meldung noch nicht alle Informationen vor, werden sie ohne unangemessene Verzögerung nachgereicht.

10.4 Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei dessen Bewertung.

10.5 Die Entscheidung über Meldungen an Aufsichtsbehörden oder betroffene Personen obliegt dem Auftraggeber, soweit keine eigene gesetzliche Pflicht des Auftragnehmers besteht.

11. NACHWEISE UND KONTROLLEN

11.1 Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung von Artikel 28 DSGVO und dieser Vereinbarung nachzuweisen.

11.2 Vorrangig können aktuelle Dokumentationen, Prüfberichte, Zertifikate oder Selbstauskünfte verwendet werden.

11.3 Der Auftraggeber darf bei berechtigtem Anlass Kontrollen selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen.

11.4 Kontrollen sind grundsätzlich mindestens zehn Werkzeuge vorher anzukündigen, während üblicher Geschäftszeiten durchzuführen und auf das erforderliche Maß zu begrenzen.

11.5 Geschäftsgeheimnisse, Daten anderer Kunden und die Sicherheit der Systeme sind zu schützen.

11.6 Ein Wettbewerber des Auftragnehmers darf nur mit dessen vorheriger Zustimmung als Prüfer eingesetzt werden.

11.7 Nachgewiesene Verstöße behebt der Auftragnehmer unverzüglich.

11.8 Angemessene Kosten einer außergewöhnlichen Kontrolle trägt der Auftraggeber, soweit die Kontrolle keinen erheblichen, vom Auftragnehmer zu vertretenden Verstoß feststellt.

12. RÜCKGABE UND LÖSCHUNG

12.1 Nach Beendigung der Leistung verarbeitet der Auftragnehmer die Auftragsdaten nicht weiter, außer soweit eine gesetzliche Aufbewahrungspflicht besteht oder die Verarbeitung zur Abwicklung der Vertragsbeendigung erforderlich ist.

12.2 Der Auftraggeber kann seine gespeicherten operativen Daten während der Vertragslaufzeit im Kundenkonto als ZIP-Datei exportieren.

12.3 Einzelheiten und aus Sicherheitsgründen ausgeschlossene Inhalte ergeben sich aus Anlage 1.

12.4 Operative Auftragsdaten werden spätestens 30 Kalendertage nach dem tatsächlichen Vertragsende gelöscht.

12.5 Daten in Sicherungskopien werden bis zum Ablauf der in Anlage 1 dokumentierten Sicherungszyklen gegen eine produktive Nutzung gesperrt und anschließend überschrieben oder gelöscht.

12.6 Gesetzliche Aufbewahrungspflichten und Nachweise über die ordnungsgemäße Verarbeitung bleiben unberührt. Solche Daten werden für andere Zwecke gesperrt.

12.7 Der Auftragnehmer bestätigt die Löschung auf Anfrage in Textform.

13. DRITTLANDÜBERMITTLUNGEN

13.1 Eine Übermittlung personenbezogener Daten außerhalb des Europäischen Wirtschaftsraums erfolgt nur auf dokumentierte Weisung des Auftraggebers oder soweit sie zur vereinbarten Leistung erforderlich und nach Kapitel V DSGVO zulässig ist.

13.2 Die jeweils eingesetzten Unterauftragnehmer, Verarbeitungsorte und Transfergrundlagen werden in Anlage 3 dokumentiert.

13.3 Fällt eine Transfergrundlage weg, informiert der Auftragnehmer den Auftraggeber und trifft eine zulässige Ersatzmaßnahme oder beendet die betroffene Übermittlung.

14. HAFTUNG

14.1 Für die Haftung der Parteien gelten Artikel 82 DSGVO und die Haftungsregelungen des Hauptvertrags, soweit diese mit zwingendem Datenschutzrecht vereinbar sind.

14.2 Jede Partei informiert die andere unverzüglich über Ansprüche, behördliche Verfahren oder sonstige Vorgänge, die die gemeinsame Vertragsdurchführung betreffen.

14.3 Die Parteien unterstützen sich im gesetzlich zulässigen Umfang bei einer abgestimmten Verteidigung.

15. LAUFZEIT UND BEENDIGUNG

15.1 Diese Vereinbarung beginnt mit ihrer gesonderten elektronischen Annahme und gilt für die Laufzeit des Hauptvertrags.

15.2 Bei der Annahme werden insbesondere folgende Angaben protokolliert:

- Dokumentart,
- Dokumentversion,
- Dokumentadresse,
- Dokumentkennung beziehungsweise Prüfsumme,
- Annahmezeitpunkt,
- zugehöriges Kundenkonto und
- verwendeter Benutzer beziehungsweise verwendete E-Mail-Adresse.

15.3 Pflichten, die ihrer Natur nach über das Vertragsende hinausreichen, insbesondere Vertraulichkeit, Löschung, Nachweis und Haftung, gelten bis zu ihrer vollständigen Erfüllung fort.

15.4 Der Auftraggeber kann den Hauptvertrag aus wichtigem Grund beenden, wenn der Auftragnehmer schwerwiegend oder wiederholt gegen diese Vereinbarung verstößt und den Verstoß nicht innerhalb einer angemessenen Frist behebt.

16. SCHLUSSBESTIMMUNGEN

16.1 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform, soweit nicht zwingendes Recht eine strengere Form verlangt.

16.2 Der Abschluss in elektronischer Form ist zulässig.

16.3 Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

16.4 Die Parteien ersetzen eine unwirksame Bestimmung durch eine rechtlich zulässige Regelung, die ihrem Zweck möglichst nahekommt.

16.5 Es gilt das Recht der Bundesrepublik Deutschland. Zwingende gesetzliche Zuständigkeiten bleiben unberührt.

ANLAGE 1 – BESCHREIBUNG DER VERARBEITUNG

1. LEISTUNG UND ZWECK

Seitenwacht überwacht im Auftrag des Auftraggebers dessen Websites auf technische Funktionsfähigkeit und Veränderungen.

Zweck ist, technische Auffälligkeiten zu erkennen, zu dokumentieren und dem Auftraggeber verständlich anzuzeigen oder zu melden.

Zum vereinbarten Leistungsumfang können insbesondere folgende Bereiche gehören:

Erreichbarkeit und Seiten

Automatisierte Aufrufe von Websites und Unterseiten sowie Erfassung von Status, Antwort, Weiterleitungen, Zeitpunkten und Prüfergebnissen.

Links, Buttons und Klickziele

Erkennen und Prüfen interner und externer Ziele sowie ausgewählter Buttons und Call-to-Actions in einem automatisierten Browser.

Formulare und E-Mail-Kontrolle

Automatisiertes Ausfüllen und Absenden ausgewählter Formulare mit synthetischen Testdaten. Prüfung von Validierung, Erfolgsmeldung, Weiterleitung und – bei entsprechender Einrichtung – technischer Bestätigung einer Testmail.

Darstellung und Performance

Automatisierte Seitenaufrufe, aktuelle Screenshots ausgewählter öffentlicher Seiten auf ausgewählten Gerätegrößen sowie Ermittlung technischer Lade- und Darstellungswerte.

SEO und Tracking

Auswertung ausgewählter technischer SEO-Merkmale und erkannter Tracking-Bausteine sowie Dokumentation feststellbarer Veränderungen.

SSL und Domainfristen

Prüfung von Zertifikatsinformationen und öffentlich verfügbaren oder manuell hinterlegten Domain- beziehungsweise Verlängerungsdaten.

Impressum und Datenschutz

Technische Kontrolle von Erreichbarkeit, Verlinkung, feststellbaren Veränderungen und erkennbaren Tracking-Angaben. Eine juristische Prüfung oder Rechtsberatung findet nicht statt.

Benachrichtigungen, Historie und Berichte

Zeitlich begrenzte Speicherung von Prüfergebnissen, Statusänderungen, Warnungen und Berichten sowie Versand von Benachrichtigungen an konfigurierte Empfänger.

Support und Sicherheit

Bearbeitung von Supportfällen, Fehleranalyse sowie Protokollierung sicherheitsrelevanter Vorgänge im erforderlichen Umfang.

2. ART DER VERARBEITUNG

Je nach Konfiguration umfasst die Verarbeitung das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Auslesen, Abfragen, Verwenden, Übermitteln, Bereitstellen, Abgleichen, Einschränken, Löschen und Vernichten personenbezogener Daten.

3. KATEGORIEN PERSONENBEZOGENER DATEN

Website- und Konfigurationsdaten

- Domain und Website-Adresse,
- Adressen öffentlicher Unterseiten,
- öffentliche Linkziele,
- Bezeichnungen,
- Prüfpläne,
- Empfänger,
- Einstellungen und
- technische Kennungen.

Monitoringdaten

- Seitentitel,
- HTTP-Statuscodes,
- Weiterleitungen,
- Ladezeiten und Performancewerte,
- technische SEO-Merkmale,
- Canonical-Angaben,
- Robots- und Indexierungsangaben,
- erkannte Tracking-Bausteine,
- SSL- und Domaininformationen sowie
- technische Ergebnisse der Rechtstextprüfung.

Prüf- und Verlaufsdaten

- Zeitpunkte und Ergebnisse der Prüfungen,
- erkannte Veränderungen,
- bestätigte Fehler,
- Warnungen,
- Berichte und
- Bearbeitungsstatus.

Formular- und Testdaten

- synthetischer Testname,
- technische Test-E-Mail-Adresse,
- automatisch erzeugte Testnachricht,
- eindeutiges Testtoken,

- Erfolgs- oder Fehlersignal,
- erkannter Empfängerstatus und
- Zeitpunkt des Tests.

Screenshots

Auf aktuellen Screenshots können öffentlich sichtbare Inhalte erscheinen, beispielsweise:

- Namen,
- Fotos,
- Kontaktdaten,
- Mitarbeiterdarstellungen und
- andere öffentlich dargestellte personenbezogene Informationen.

Protokoll- und Sicherheitsdaten

- Zeitpunkte von Anmeldungen,
- Profil- und Passwortänderungen,
- Datenexporte,
- Website-Löschungen,
- AVV-Annahmen,
- administrative Kundenansichten,
- technische Fehler und
- ein nicht rückrechenbarer Fingerabdruck der zugreifenden Adresse.

Support- und Kommunikationsdaten

Support- und Kommunikationsdaten werden verarbeitet, soweit sie zur Bearbeitung des konkreten Vorgangs erforderlich sind.

Datenminimierung

Werte von URL-Parametern und URL-Fragmente werden vor der dauerhaften Speicherung entfernt.

Rohe IP-Adressen werden in Sicherheitsprotokollen nicht dauerhaft gespeichert. Stattdessen wird ein mit einem geheimen Systemwert gebildeter, nicht rückrechenbarer Fingerabdruck verwendet.

4. FORMULARTESTS UND POSTFACHVERBINDUNGEN

Bei Formulartests werden ausschließlich automatisch erzeugte Testdaten eingesetzt.

Seitenwacht speichert keine echten Kundenanfragen der überwachten Website.

Der Inhalt eingehender E-Mails wird nicht dauerhaft gespeichert.

Eine Verbindung zu Microsoft 365 oder Google Mail wird nur eingerichtet, wenn der Auftraggeber dies ausdrücklich auswählt.

OAuth-Zugangsdaten werden verschlüsselt gespeichert.

Serverseitig wird gezielt nach dem eindeutigen Seitenwacht-Testtoken gesucht. Unbeteiligte Nachrichten sollen nicht heruntergeladen werden.

Von passenden Testnachrichten werden nur die für die Zustellbestätigung erforderlichen Metadaten verarbeitet.

Der Auftraggeber kann die Postfachverbindung trennen.

Alternativ kann eine Weiterleitungs- oder WordPress-Verbindung zur technischen Bestätigung der Formularzustellung verwendet werden.

5. KATEGORIEN BETROFFENER PERSONEN

Abhängig von der überwachten Website können Daten folgender Personen verarbeitet werden:

- Kunden und Interessenten des Auftraggebers,
- Websitebesucher,
- Beschäftigte, freie Mitarbeitende und Ansprechpartner des Auftraggebers oder seiner Kunden,
- öffentlich genannte Ansprechpartner,
- sonstige Personen, deren Daten auf überwachten öffentlichen Seiten sichtbar sind,
- Empfänger von Formulartests, Benachrichtigungen und Berichten sowie
- Nutzer des Seitenwacht-Kundenkontos.

6. BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN

Die Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 DSGVO, insbesondere Gesundheitsdaten, sowie von Daten über strafrechtliche Verurteilungen und Straftaten ist nicht Bestandteil der vereinbarten Leistung.

Der Auftraggeber darf Seitenwacht nicht gezielt zur Verarbeitung entsprechender Daten einsetzen.

7. DAUER UND LÖSCHKONZEPT

Die Verarbeitung dauert grundsätzlich für die Laufzeit des Hauptvertrags.

Es gelten folgende Lösch- und Aufbewahrungsfristen:

Operative Konto-, Website- und Prüfdaten nach Vertragsende

Automatische Löschung spätestens 30 Kalendertage nach dem tatsächlichen Vertragsende. Dazu gehören insbesondere Kundenkonto, Websites, Formulare, Prüfergebnisse, Screenshots, Konfigurationen, Postfachverbindungen und Monitoringhistorien.

Prüfhistorien

- Basic: 7 Tage,
- Pro: 30 Tage,
- Scale: 180 Tage beziehungsweise sechs Monate.

Die Begrenzung wird durch eine tägliche Löschroutine technisch durchgesetzt.

Aktuelle Screenshots

Bis zur Ersetzung beziehungsweise Löschung der Website oder des Kundenkontos.

Berichte

12 Monate.

Technische Anwendungsfehler

30 Tage.

Sicherheits- und Administratorprotokolle

180 Tage.

Abgeschlossene E-Mail-Wiederherstellungsanträge

180 Tage.

Pseudonymisierte Missbrauchsnachweise

730 Tage für kostenlose Checks und mehrfach verwendete Testdomains.

Abgelaufene technische WordPress-Prüfanfragen

Ein zusätzlicher Tag.

Supportanfragen per E-Mail

Organisatorisch höchstens 12 Monate, soweit keine längere Aufbewahrung für einen konkreten Vorgang erforderlich ist.

Hetzner-Serverbackups

Täglich werden sieben rotierende Sicherungsstände vorgehalten. Bereits gelöschte Daten können deshalb noch ungefähr sieben Tage in einem Serverbackup enthalten sein und werden anschließend durch die Rotation überschrieben.

Manuelle verschlüsselte Notfall-Backups

Spätestens 30 Tage nach der Erstellung.

Vertrags-, Rechnungs- und Annahmenachweise

Diese Nachweise dürfen getrennt von den operativen Auftragsdaten nach den anwendbaren gesetzlichen Aufbewahrungs- und Nachweispflichten gespeichert bleiben. Die Verarbeitung erfolgt in eigener Verantwortlichkeit von Seitenwacht.

8. EXPORT UND LÖSCHUNG DURCH DEN AUFTRAGGEBER

Der Auftraggeber kann seine gespeicherten operativen Daten im Kundenkonto als ZIP-Datei exportieren.

Der Export enthält keine:

- Passwort-Hashes,
- OAuth-Zugangstoken,
- WordPress-Verbindungsschlüssel,
- Reset-Token,
- Verifizierungsschlüssel oder
- sonstigen Zugangsschlüssel.

Der Auftraggeber kann eine einzelne Website einschließlich der zugehörigen Prüfdaten und Screenshots selbst dauerhaft löschen.

Dafür sind die Eingabe des Website-Namens und des aktuellen Passworts erforderlich.

Die Startseite oder einzelne alte Einträge können innerhalb der vorgesehenen Oberfläche aus der laufenden Überwachung entfernt werden.

9. VERARBEITUNG IN EIGENER VERANTWORTLICHKEIT VON SEITENWACHT

Nicht Gegenstand dieser Auftragsverarbeitung sind Daten, die Seitenwacht für eigene Vertrags-, Abrechnungs-, Sicherheits- und gesetzliche Nachweiszwecke verarbeitet.

Dazu können insbesondere gehören:

- Unternehmensname,
- Ansprechpartner,
- Login-E-Mail-Adresse,
- gebuchter Tarif,
- Abrechnungszeitraum,
- Vertrags- und Zahlungsstatus sowie
- Nachweise über die Annahme von AGB, Datenschutzerklärung und AVV.

Für diese Verarbeitungen ist Seitenwacht selbst Verantwortlicher. Die Einzelheiten ergeben sich aus der Datenschutzerklärung und dem eigenen Löschkonzept.

10. TECHNISCHE UND RECHTLICHE ABGRENZUNG

Seitenwacht ist ein technisches Überwachungswerkzeug.

Die Prüfung von Impressum und Datenschutzerklärung beschränkt sich auf technisch erkennbare Merkmale, Erreichbarkeit, Verlinkung und feststellbare Veränderungen.

Seitenwacht garantiert nicht:

- die vollständige rechtliche Richtigkeit eines Impressums,
- die vollständige rechtliche Richtigkeit einer Datenschutzerklärung,
- die dauerhafte Fehlerfreiheit einer Website,
- die tatsächliche Zustellung jeder externen E-Mail,
- die vollständige Erkennung jedes Tracking-Dienstes oder
- die rechtliche Konformität der überwachten Website.

Technische Hinweise und Prüfergebnisse ersetzen keine Rechtsberatung, Datenschutzberatung oder manuelle fachliche Prüfung.

ANLAGE 2 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. TRANSPORTVERSCHLÜSSELUNG UND SITZUNGEN

- HTTPS/TLS über Caddy für app.seitenwacht.de,
- sichere Verbindung zur Anwendung und
- sichere und HTTP-only Sitzungs-Cookies im Produktivbetrieb.

2. PASSWORTSCHUTZ

- Passwörter werden nicht im Klartext gespeichert.
- Passwort-Hashes werden mit PBKDF2-SHA256 und 310.000 Iterationen erstellt.
- Passwort-Zurücksetzungen erfolgen über zeitlich begrenzte Links.
- Änderungen der Login-E-Mail werden durch Sicherheitsbestätigungen abgesichert.
- Wenn der Zugriff auf die bisherige Adresse fehlt, ist ein gesonderter Wiederherstellungsprozess vorgesehen.

3. MANDANTENTRENNUNG

- Jedes Kundenkonto ist einer eigenen Organisation zugeordnet.
- Kundenabfragen werden serverseitig auf diese Organisation begrenzt.
- Kunden können nicht auf Websites, Formulare oder Prüfergebnisse anderer Kunden zugreifen.
- Administrative Kundenansichten durch die Betreiberin werden protokolliert.

4. SCHUTZ DER ANWENDUNG

- CSRF-Schutz,
- Same-Origin-Prüfung,
- Begrenzung der Anfragegrößen,
- Begrenzung wiederholter Loginversuche,
- Schutz vor Zugriffen auf interne oder lokale Netzwerkziele,
- sichere Prüfung von Weiterleitungen und
- abgesicherte Browser- und Websiteabrufe.

5. CONTAINER-HÄRTUNG

- keine zusätzlichen Linux-Rechte für Anwendungscontainer,
- no-new-privileges,
- Prozessbegrenzungen,
- automatische Neustarts und
- größenbegrenzte, rotierende Docker-Protokolle.

6. TOKEN UND ZUGANGSDATEN

- OAuth- und WordPress-Verbindungstoken werden verschlüsselt gespeichert.
- Zugangsschlüssel werden vom Datenexport ausgeschlossen.
- Zugriffe werden auf den technisch erforderlichen Umfang beschränkt.

7. DATENBANK UND SPEICHER

Die laufende SQLite-Datenbank besitzt keine zusätzliche anwendungsseitige Vollverschlüsselung.

Der Zugriff ist durch Server-, Betriebssystem- und Containerrechte beschränkt.

8. SICHERUNGEN

- tägliche Hetzner-Serverbackups mit sieben rotierenden Sicherungsständen,
- symmetrische Verschlüsselung manueller externer Datenbanksicherungen mit AES-256 und
- Löschung manueller Notfall-Backups spätestens nach 30 Tagen.

9. DATENMINIMIERUNG

- Verwendung synthetischer Formulartestdaten,
- Token-Suche statt dauerhafter Speicherung vollständiger E-Mails,
- Entfernung von URL-Parameterwerten und URL-Fragmenten vor der dauerhaften Speicherung,
- keine planmäßige Verarbeitung besonderer Kategorien personenbezogener Daten und
- Ausschluss von Zugangsschlüsseln aus Kundenexporten.

10. PROTOKOLLIERUNG

Protokolliert werden insbesondere:

- erfolgreiche Anmeldungen,
- Profiländerungen,
- Passwortänderungen,
- Datenexporte,
- Website-Löschungen,
- AVV-Annahmen und
- administrative Kundenansichten.

Rohe IP-Adressen werden nicht dauerhaft gespeichert. Stattdessen wird ein mit einem geheimen Systemwert gebildeter, nicht rückrechenbarer Fingerabdruck verwendet.

11. LÖSCHUNG

- tägliche Löschr- und Aufbewahrungsroutine,
- Selbstlöschung einzelner Websites durch den Auftraggeber,
- automatische Löschung operativer Daten spätestens 30 Tage nach dem tatsächlichen Vertragsende und
- Überschreibung gelöschter Daten in Backups entsprechend der dokumentierten Rotation.

12. UPDATES UND BETRIEB

- regelmäßige Aktualisierung der Anwendung,
- regelmäßige Sicherheitsupdates verwendeter Komponenten,
- automatische Gesundheitskontrolle der laufenden Container und
- kontrollierte Durchführung technischer Änderungen.

13. AUFTRAGSKONTROLLE

- Verarbeitung nur auf dokumentierte Weisung,
- geregelter Support- und Administratorzugriff,
- Auswahl und vertragliche Einbindung eingesetzter Unterauftragnehmer und
- Protokollierung administrativer Kundenansichten.

14. PRODUKTIVE TECHNISCHE UMGEBUNG

Anwendung und Hostingregion

app.seitenwacht.de auf Hetzner-Infrastruktur in nbg1, Nürnberg, Deutschland.

Datenbank

SQLite auf dem Anwendungsserver. Es besteht keine zusätzliche anwendungsseitige Vollverschlüsselung.

Sicherungsintervall

Täglich mit sieben rotierenden Hetzner-Sicherungsständen.

Kontakt für Sicherheitsvorfälle

datenschutz@seitenwacht.de

ANLAGE 3 – GENEHMIGTE UNTERAUFTRAGNEHMER

1. HETZNER

Anbieter:

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Deutschland

Leistung:

- Betrieb von app.seitenwacht.de,
- Hosting der Anwendung,
- Hosting der SQLite-Datenbank,
- Speicherung aktueller Screenshots,
- Serverbetrieb und
- Serverbackups.

Verarbeitete Daten:

Die in Anlage 1 bezeichneten operativen Auftragsdaten.

Verarbeitungsort:

nbg1, Nürnberg, Deutschland.

Drittlandtransfer:

Für die bezeichnete Hostingregion ist keine Drittlandübermittlung vorgesehen.

2. BREVO

Anbieter:

Brevo GmbH
Köpenicker Str. 126
10179 Berlin
Deutschland

Eingetragen beim Amtsgericht Berlin-Charlottenburg unter HRB 133191.

Leistung:

Versand von:

- Konto-E-Mails,
- Passwort- und Sicherheits-E-Mails,
- Warnmeldungen,
- Berichten und
- Begrüßungsmails.

Verarbeitete Daten:

- Empfängeradresse,
- Betreff,
- Inhalt der versendeten Systemmail sowie
- Versand- und Zustellstatus.

Verarbeitungsorte und Drittlandübermittlungen:

Die Verarbeitung erfolgt durch Brevo und die im jeweils aktuellen Data Processing Agreement aufgeführten Unterauftragnehmer. Soweit Daten außerhalb des Europäischen Wirtschaftsraums verarbeitet werden, erfolgen Übermittlungen auf Grundlage der im Brevo-DPA bezeichneten Garantien, insbesondere Angemessenheitsbeschlüssen, dem EU-US Data Privacy Framework oder Standardvertragsklauseln mit ergänzenden Schutzmaßnahmen.

Vertragsgrundlage:

Data Processing Agreement gemäß Anlage 3 der Brevo Terms of Service in der jeweils für das Seitenwacht-Konto geltenden Fassung.

3. VOM AUFTRAGGEBER AUSGEWÄHLTE POSTFACHANBIETER

Microsoft 365 oder Google Mail werden nur angebunden, wenn der Auftraggeber selbst eine entsprechende Postfachverbindung einrichtet.

Diese Anbieter werden damit nicht automatisch von Seitenwacht als Unterauftragnehmer für alle Kunden eingesetzt.

Der Auftraggeber ist für die Zulässigkeit seiner Verbindung und das Vertragsverhältnis zu seinem Postfachanbieter verantwortlich.

Seitenwacht verarbeitet über die Verbindung ausschließlich die in Anlage 1 beschriebenen Testtoken- und Zustellinformationen.

4. DIENSTE AUSSERHALB DER AUFTRAGSVERARBEITUNG

Stripe verarbeitet Zahlungs-, Rechnungs- und Abonnementdaten.

Stripe erhält keine überwachten Website-Inhalte, Screenshots oder Formulartestergebnisse. Die Rolle von Stripe im Zahlungsprozess wird getrennt in der Datenschutzerklärung und den Zahlungsbedingungen beschrieben.

Derzeit werden innerhalb der Seitenwacht-Anwendung keine externen Anbieter für folgende Aufgaben eingesetzt:

- externe Fehlerprotokollierung,
- externe Anwendungsanalyse,
- externes Support- oder Ticketsystem oder
- externe Datenbank außerhalb des Hetzner-Servers.

5. ÄNDERUNGEN BEI UNTERAUFTRAGNEHMERN

Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen entsprechend Ziffer 7 dieser Vereinbarung.

Die Information erfolgt über die im Kundenkonto hinterlegte geschäftliche E-Mail-Adresse.

ANLAGE 4 – WEISUNGEN, KONTAKTE UND ELEKTRONISCHE ANNAHME

1. KONTAKTE DES AUFTRAGNEHMERS

Vertragskontakt:

kontakt@seitenwacht.de

Datenschutzkontakt:

datenschutz@seitenwacht.de

Kontakt für Sicherheitsvorfälle:

datenschutz@seitenwacht.de

Weisungsberechtigte Person beim Auftragnehmer:

Anna-Lena Meyringer

2. KONTAKTE DES AUFTRAGGEBERS

Die Vertrags-, Datenschutz- und Weisungskontakte des Auftraggebers ergeben sich aus den bei Vertragsschluss und im Kundenkonto hinterlegten Daten.

Der Auftraggeber ist dafür verantwortlich, diese Kontaktdaten aktuell zu halten.

3. DOKUMENTIERTE WEISUNGEN

Die anfänglichen Weisungen ergeben sich aus dem Hauptvertrag, dieser Vereinbarung und der Konfiguration des Auftraggebers im Kundenkonto.

Zusätzliche Weisungen sollen in Textform über die angegebenen Kontakte erteilt und von beiden Parteien nachvollziehbar dokumentiert werden.

Der Auftraggeber ist insbesondere verantwortlich für:

- die Rechtmäßigkeit der Überwachung,
- die Auswahl der überwachten Websites,
- die Einrichtung von Formulartests,
- die Richtigkeit hinterlegter Empfänger,
- erforderliche Weisungen oder Berechtigungen seiner eigenen Kunden,
- die Vermeidung besonderer Kategorien personenbezogener Daten und
- die Rechtmäßigkeit einer Postfachverbindung.

4. ELEKTRONISCHE ANNAHME UND NACHWEIS

Der AVV wird unter <https://seitenwacht.de/avv> bereitgestellt.

Er wird beim Kauf getrennt von den AGB und der Datenschutzerklärung elektronisch angenommen.

Gespeichert werden:

- Art des angenommenen Dokuments,
- Dokumentversion,
- Dokumentadresse,
- Dokumentkennung beziehungsweise SHA-256-Prüfsumme,
- Annahmezeitpunkt,
- zugehöriges Kundenkonto sowie
- Benutzer beziehungsweise verwendete E-Mail-Adresse.

Die angenommene Fassung bleibt im Bereich „Konto & Tarif“ abrufbar.

Ältere oder manuell angelegte Kundenkonten können den AVV dort nachträglich annehmen.

Die elektronische Annahme genügt zum Abschluss dieser Vereinbarung. Eine zusätzliche handschriftliche Unterschrift ist nicht erforderlich.