> **Entwurf – anwaltlich nicht geprüft.** Dieser Text ist eine Arbeitsgrundlage, kein geprüftes Vertragsmuster. Vor der Unterzeichnung gehört er in die Hände einer Anwältin oder eines Anwalts. Stellen, die noch auszufüllen sind, stehen in eckigen Klammern.
>
> **Stand der Umsetzung:** Die Überwachung von Domain-Einträgen und die Auswertung von DMARC-Berichten sind zum Stand dieses Entwurfs noch nicht in Betrieb. In Betrieb ist der einmalige Domain-Check und die Warteliste. Der Vertrag beschreibt den vereinbarten Leistungsumfang; was davon schon läuft, ist im Einzelfall zu prüfen.

1. Parteien

Verantwortlicher (nachfolgend „Kunde"): [Firma, Anschrift, vertreten durch]

Auftragsverarbeiter: Finden & Verbinden GmbH, Schumannstraße 27, 60325 Frankfurt am Main, vertreten durch den Geschäftsführer Alexander Penner, eingetragen beim Amtsgericht Frankfurt am Main unter HRB 140041.

Dieser Vertrag konkretisiert die Pflichten aus Art. 28 DSGVO für die Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter im Auftrag des Kunden vornimmt.

2. Gegenstand und Zweck

Der Auftragsverarbeiter erbringt für den Kunden folgende Leistungen:

- **Überwachung von Domain-Einträgen.** Wiederkehrende Abfrage öffentlicher DNS-Einträge der vom Kunden benannten Domains (MX, SPF, DKIM, DMARC, MTA-STS, TLS-RPT), Bewertung nach den einschlägigen Standards (RFC 5321, 7208, 6376, 7489, 8461, 8460) und Benachrichtigung bei Änderungen.
- **Auswertung von DMARC-Berichten.** Entgegennahme der aggregierten Berichte, die Empfänger an eine vom Kunden hinterlegte Adresse senden, Aufbereitung zu einer verständlichen Übersicht sendender Dienste.

Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt.

3. Art der Daten und Kreis der Betroffenen

Datenarten

- Domainnamen des Kunden und die dazu öffentlich hinterlegten DNS-Einträge
- Prüfergebnisse und deren zeitlicher Verlauf
- Kontaktdaten der beim Kunden zuständigen Personen: E-Mail-Adresse, gegebenenfalls Name und Rolle
- Aus DMARC-Berichten: IP-Adressen sendender Systeme, Angaben zum Ergebnis der Prüfung von SPF und DKIM, Anzahl der Nachrichten je Sendequelle

Kreis der Betroffenen

- Beschäftigte und Beauftragte des Kunden, soweit sie als Ansprechpartner hinterlegt sind
- Inhaber der IP-Adressen, die in DMARC-Berichten als sendende Systeme auftauchen

Nicht Gegenstand der Verarbeitung sind Inhalte von E-Mails, Betreffzeilen, Empfängeradressen einzelner Nachrichten sowie Zugangsdaten zu Systemen des Kunden. Der Auftragsverarbeiter benötigt und erhält keinen Zugang zu Postfächern des Kunden.

4. Dauer

Der Vertrag beginnt mit der Beauftragung und läuft, solange der Kunde die Leistung nutzt. Er endet mit dem Hauptvertrag. Die Pflichten zur Löschung (Ziffer 8) und zur Vertraulichkeit gelten über das Ende hinaus fort.

5. Weisungen

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden. Weisungen ergehen in Textform an kontakt@mailverity.de; mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies dem Kunden unverzüglich mit und darf ihre Ausführung bis zur Klärung aussetzen.

Der Auftragsverarbeiter unterrichtet den Kunden unverzüglich, wenn er von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt, und unterstützt ihn bei den Pflichten aus Art. 33 und 34 DSGVO sowie bei Anfragen betroffener Personen (Art. 12 bis 23 DSGVO).

6. Technische und organisatorische Maßnahmen

Die Maßnahmen sind in **Anlage 1** beschrieben. Der Auftragsverarbeiter darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.

7. Unterauftragsverarbeiter

Der Kunde stimmt dem Einsatz der folgenden Unterauftragsverarbeiter zu. Ein Wechsel oder die Aufnahme weiterer wird mindestens vier Wochen vorher in Textform angekündigt; der Kunde kann innerhalb dieser Frist widersprechen.

Unternehmen	Sitz	Ort der Verarbeitung	Zweck
Hetzner Online GmbH	Gunzenhausen, Deutschland	Deutschland	Betrieb von Anwendung und Datenbank

Unternehmen	Sitz	Ort der Verarbeitung	Zweck
Brevo (Sendinblue GmbH)	Paris, Frankreich	Europäische Union	Versand von System- und Benachrichtigungsmails
Plausible Insights OÜ	Tallinn, Estland	Europäische Union	Reichweitenmessung der Website, ohne Cookies und ohne personenbezogene Daten

Hinweis: Alle drei Unterauftragsverarbeiter haben ihren Sitz in der Europäischen Union und verarbeiten dort; ein Drittlandtransfer im Sinne von Kapitel V DSGVO findet nicht statt. Die genaue vertragschließende Gesellschaft von Brevo ist vor Unterzeichnung zu bestätigen – die Unternehmensgruppe führt mehrere Gesellschaften.

8. Löschung nach Vertragsende

Nach Ende des Vertrags löscht der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten innerhalb von 30 Tagen, sofern der Kunde nicht ausdrücklich die Rückgabe verlangt. Bestehende gesetzliche Aufbewahrungspflichten bleiben unberührt; die betroffenen Daten werden in diesem Fall in der Verarbeitung eingeschränkt und nach Ablauf der Frist gelöscht.

Die Löschung wird dem Kunden auf Verlangen in Textform bestätigt. Sicherungskopien werden im Rahmen des üblichen Sicherungszyklus überschrieben; ein gezielter Zugriff auf sie findet nicht statt.

9. Kontrollrechte

Der Kunde hat das Recht, die Einhaltung dieses Vertrags zu überprüfen. Der Auftragsverarbeiter erteilt dazu auf Anfrage in Textform Auskunft und stellt die Beschreibung der technischen und organisatorischen Maßnahmen zur Verfügung.

Reicht das nicht aus, kann der Kunde nach Ankündigung mit angemessener Frist – in der Regel vier Wochen – während der üblichen Geschäftszeiten eine Prüfung vor Ort vornehmen oder durch einen zur Verschwiegenheit verpflichteten Dritten vornehmen lassen, der nicht Wettbewerber des Auftragsverarbeiters ist. Die Prüfung darf den Betrieb nicht unangemessen beeinträchtigen. Aufwand über eine Prüfung je Kalenderjahr hinaus kann der Auftragsverarbeiter nach Aufwand berechnen.

Anlage 1: Technische und organisatorische Maßnahmen

Diese Anlage beschreibt, was tatsächlich eingerichtet ist oder vor Inbetriebnahme eingerichtet wird. Punkte, die noch offen sind, sind als solche gekennzeichnet.

Vertraulichkeit

- **Zutritt.** Die Server stehen in Rechenzentren der Hetzner Online GmbH in Deutschland. Für die physische Sicherung gelten deren Maßnahmen; ein eigener Zutritt besteht nicht.
- **Zugang.** Der Zugriff auf Server und Datenbank erfolgt ausschließlich über Schlüsselpaare, nicht über Passwörter. Die Anwendung lauscht nur auf der lokalen Schnittstelle und ist von außen ausschließlich über den vorgelagerten Reverse Proxy erreichbar.
- **Zugriff.** Die Anwendung verwendet einen eigenen Datenbankbenutzer. Geheimnisse (Datenbankzugang, Schlüssel für Pseudonymisierung und Abmeldelinks, Zugangsschlüssel des Mailversands) stehen ausschließlich in der Umgebung, nie im Quelltext; ein fehlender oder zu kurzer Schlüssel führt zum Startabbruch.
- **Trennung.** Prüfergebnisse und Kontaktdaten liegen in getrennten Tabellen. Ein Prüfergebnis enthält keinen Personenbezug außer dem Domainnamen.

Datenminimierung

- **Keine IP-Adressen.** Die Adresse des Aufrufers wird nicht gespeichert. Für die Begrenzung der Anfragen wird sie mit einem täglich wechselnden Schlüssel in einen nicht rückrechenbaren Wert überführt; dieser Wert liegt ausschließlich im Arbeitsspeicher und wird nirgends abgelegt.
- **Keine Mailinhalte.** Es werden keine Nachrichteninhalte verarbeitet.
- **Keine Zugangsdaten.** Die Prüfung nutzt ausschließlich öffentlich abrufbare Einträge.
- **Sprechende Fehlermeldungen ohne Daten.** Protokolleinträge enthalten weder E-Mail-Adressen noch Bestätigungstoken.

Integrität

- **Transport.** Der Zugriff auf die Website erfolgt ausschließlich über TLS.
- **Bestätigungslinks.** Wartelisten-Einträge werden über ein Double-Opt-in bestätigt. Der Bestätigungstoken besteht aus 32 zufälligen Byte und liegt in der Datenbank nur als SHA-256-Hash; er gilt 72 Stunden und lässt sich genau einmal einlösen.
- **Abmeldelinks.** Die Signatur der Abmeldelinks wird aus einem eigenen Serverschlüssel abgeleitet und nicht gespeichert.
- **Eingabeprüfung.** Eingaben werden serverseitig geprüft; Datenbankzugriffe erfolgen ausschließlich mit gebundenen Parametern.

Verfügbarkeit und Belastbarkeit

- **Sicherung.** Tägliche Sicherung der Datenbank. (Vor Inbetriebnahme einzurichten; Aufbewahrungsdauer und Wiederherstellungstest sind festzulegen.)

- **Begrenzung.** Anfragen werden je Aufrufer begrenzt, ebenso der Versand von Bestätigungsmails je Empfängerpostfach und insgesamt.
- **Wiederherstellung.** Die Anwendung ist zustandslos und aus dem Quelltext reproduzierbar; der Zustand liegt vollständig in der Datenbank.

Löschung

- **Prüfergebnisse** werden nach 30 Tagen gelöscht.
- **Unbestätigte Wartelisten-Einträge** werden nach 72 Stunden gelöscht.
- **Bestätigte Einträge** bleiben bis zum Widerruf; in jeder Mail steht ein Abmeldelink, der die Zeile ohne Rückfrage löscht.
- Beide Fristen werden durch geplante Aufgaben auf dem Server durchgesetzt. (Vor Inbetriebnahme einzurichten – ohne sie sind die Fristen nicht eingehalten.)

Nachvollziehbarkeit

- Änderungen am Quelltext laufen über Pull Requests mit automatischer Prüfung (Typprüfung, Stilprüfung, Testlauf, Migrationsprüfung) und sind in der Versionsverwaltung vollständig nachvollziehbar.
- Änderungen an der Prüflogik erfordern Tests mit echten DNS-Fixtures.

Auftragskontrolle

- Unterauftragsverarbeiter sind in Ziffer 7 benannt. Verträge nach Art. 28 DSGVO sind mit ihnen zu schließen. (Status je Anbieter vor Inbetriebnahme zu dokumentieren.)