Auftragsverarbeitungsvertrag (AVV)

Auftragsverarbeitung nach Art. 28 DSGVO · Stand: 10. November 2026

zwischen dem **Verantwortlichen** (Kunde/Veranstalter)

Name/Firma: _____
Anschrift: _____
Vertreten durch: _____

und dem **Auftragsverarbeiter**

Prof. Dr. Niels Van Quaquebeke · Sealed — Letter to My Future Self
Simplonstraße 16, 10245 Berlin, Deutschland · sealed@quaquebeke.de

§ 1 Gegenstand und Dauer

Der Auftragsverarbeiter stellt die Web-Anwendung „Sealed“ (futureme.quaquebeke.de) bereit, mit der Teilnehmende von Veranstaltungen des Verantwortlichen Briefe an ihr zukünftiges Ich schreiben, die zu einem selbst gewählten Zeitpunkt per E-Mail zugestellt werden. Dieser Vertrag gilt für die Dauer der Nutzung der Anwendung durch den Verantwortlichen und endet mit der vollständigen Löschung der Daten nach § 7.

§ 2 Art und Zweck der Verarbeitung

Erhebung, verschlüsselte Speicherung, terminierte E-Mail-Zustellung und anschließende Löschung von Briefen der Teilnehmenden; Bereitstellung aggregierter Kennzahlen (geplant/zugestellt/fehlgeschlagen) für den Verantwortlichen. Eine Nutzung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt; Briefinhalte sind dem Verantwortlichen zu keinem Zeitpunkt zugänglich.

§ 3 Datenkategorien und betroffene Personen

Kategorien: E-Mail-Adresse, optional Name und Betreff, Brieftext (verschlüsselt gespeichert), optionale Anhänge (Fotos, Dokumente), Sprach- und Zustell-Metadaten, technische Protokolldaten. Betroffene: Teilnehmende der Veranstaltungen des Verantwortlichen sowie von Teilnehmenden benannte Kopie-Empfänger.

§ 4 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Vertrags und der dokumentierten Funktionsweise der Anwendung (Art. 28 Abs. 3 lit. a DSGVO); zur Vertraulichkeit verpflichtete Personen (lit. b); trifft die technischen und organisatorischen Maßnahmen der Anlage 1 (Art. 32, lit. c); unterstützt den Verantwortlichen bei Betroffenenrechten und den Pflichten aus Art. 32–36 (lit. e, f); meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis; führt nach Vertragsende die Löschung nach § 7 durch (lit. g) und stellt die Informationen nach lit. h bereit. Automatische Löschfristen der Anwendung: Brieftexte werden mit der Zustellung gelöscht, Anhänge 30 Tage nach Zustellung, unbestätigte Briefe nach 72 Stunden.

§ 5 Unterauftragsverarbeiter

Die in Anlage 2 genannten Unterauftragsverarbeiter gelten als genehmigt. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen; der Verantwortliche kann aus wichtigem Grund widersprechen. Eine Verarbeitung findet ausschließlich in der Europäischen Union statt.

§ 6 Weisungsrecht

Weisungen ergeben sich aus der Konfiguration der Anwendung durch den Verantwortlichen (Events, Schließdaten, Branding, Export). Darüber hinausgehende Weisungen bedürfen der Textform an sealed@quaquebeke.de.

§ 7 Löschung und Rückgabe

Nach Ende der Nutzung löscht der Auftragsverarbeiter alle personenbezogenen Daten des Verantwortlichen, soweit keine gesetzlichen Aufbewahrungspflichten bestehen. Noch nicht zugestellte Briefe werden zugestellt, sofern der Verantwortliche nichts anderes verlangt – die Zustellung versiegelter Briefe ist Kern der Leistung gegenüber den Betroffenen. Sicherungskopien rotieren automatisch nach 7 Tagen aus.

§ 8 Nachweise und Kontrollen

Der Auftragsverarbeiter weist die Einhaltung dieses Vertrags durch Dokumentation der Maßnahmen nach Anlage 1 nach. Kontrollen vor Ort sind nach Ankündigung mit angemessener Frist während üblicher Geschäftszeiten möglich, soweit sie den Schutz der Daten Dritter nicht gefährden.

§ 9 Schlussbestimmungen

Es gilt deutsches Recht. Nebenabreden bedürfen der Textform. Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Bei Widersprüchen zu Nutzungs- oder Leistungsvereinbarungen geht dieser AVV in datenschutzrechtlichen Fragen vor.

Ort, Datum, Unterschrift Verantwortlicher	Ort, Datum, Unterschrift Auftragsverarbeiter

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Verschlüsselung & Vertraulichkeit: Brieftexte werden mit modernen Verfahren (libsodium XSalsa20-Poly1305, ersatzweise AES-256-GCM) verschlüsselt gespeichert; der Schlüssel liegt ausschließlich auf dem Server. Transport ausschließlich über TLS (HTTPS). Veranstalter sehen technisch bedingt nur Kennzahlen, nie Inhalte.
Zugriffskontrolle: Konten ausschließlich über Einmal-Anmeldelinks (Magic-Link, Einmal-Token, atomare Entwertung); rollenbasierte Trennung (Admin/Host); Mandantentrennung auf Datenebene je Konto und Event.
Datensparsamkeit & Löschung: keine Werbe-Tracker, keine Analyse-Cookies; automatische Löschung: Brieftext bei Zustellung, Anhänge 30 Tage nach Zustellung, unbestätigte Briefe nach 72 Stunden, Medien-Dateien nach dem letzten zugehörigen Brief.
Verfügbarkeit: tägliche automatische Datenbank-Sicherung (7 Tage Vorhaltung), Zustell-Überwachung mit Wiederholversuchen, technischer Wächter mit Alarmierung des Betreibers.
Missbrauchs-Schutz: Ratenbegrenzung, Honeypot-Felder, Double-Opt-in für alle frei erreichbaren Formulare, Mengenbegrenzung je Empfänger-Adresse.

Anlage 2 — Genehmigte Unterauftragsverarbeiter

domainfactory GmbH, Ismaning, Deutschland — Hosting der Anwendung, Speicherung der Daten, E-Mail-Versand. Verarbeitung ausschließlich in Rechenzentren in Deutschland.

Hinweis: Dieses Muster wurde mit Sorgfalt erstellt, ersetzt aber keine Rechtsberatung im Einzelfall.