TOMS, UNTERAUFTRAGS-VERARBEITER & LÖSCHINFOS

Technische und organisatorische Maßnahmen, Unterauftragsverarbeiterliste sowie Lösch- und Drittlandinformationen

DOKUMENT	TOMs / Unterauftragsverarbeiter / Lösch- und Drittlandinformationen
ANBIETER	Logical Optimized Orchestrated Processing Model & Stoppa GbR
RECHTSFORM	Gesellschaft bürgerlichen Rechts
GESELLSCHAFTER	Lucian Stoppa und Anton Model
ANSCHRIFT	Hans-Sachs-Str. 51, 03046 Cottbus
GELTUNG	soweit im jeweiligen Projekt eingesetzt
FASSUNG	Version 1.1 - Stand: 07.06.2026

Hinweis zur Projektbezogenheit: Nicht jeder genannte Anbieter wird automatisch in jedem Projekt eingesetzt. Maßgeblich ist der tatsächliche projektbezogene Einsatz laut Angebot oder Leistungsbeschreibung.

Hinweis: Diese Druckfassung dient der professionellen Bereitstellung und Unterzeichnung. Maßgeblich ist die jeweils in den Vertrag einbezogene Fassung mit Version und Stand.

1. Technische und organisatorische Maßnahmen

Diese technischen und organisatorischen Maßnahmen beschreiben die Standardmaßnahmen der Logical Optimized Orchestrated Processing Model & Stoppa GbR zum Schutz personenbezogener Daten im Rahmen von Kundenprojekten.

Soweit in diesem Dokument die Bezeichnung „L.O.O.P." verwendet wird, handelt es sich um eine Marke bzw. geschäftliche Bezeichnung der Logical Optimized Orchestrated Processing Model & Stoppa GbR.

Die konkreten Maßnahmen können je nach Projekt, eingesetzten Systemen, Hostingumgebung, Kundenanforderungen und technischen Rahmenbedingungen angepasst oder ergänzt werden.

Diese TOMs konkretisieren die Sicherheitsmaßnahmen zum Auftragsverarbeitungsvertrag. Leistungspflichten, Support, Verfügbarkeit, Haftung, Nutzungsrechte und wirtschaftliche Regelungen ergeben sich aus dem jeweiligen Angebot, den AGB und gegebenenfalls einem gesonderten SLA.

2. Vertraulichkeit

L.O.O.P. beschränkt den Zugriff auf personenbezogene Daten auf berechtigte Personen, die den Zugriff zur Durchführung des jeweiligen Projekts benötigen.

Maßnahmen können insbesondere sein:

- Zugriff nur für berechtigte Gesellschafter, Mitarbeiter, Freelancer oder projektbezogene Beteiligte
- rollen- und rechtebasierte Zugriffsbeschränkungen, soweit technisch möglich
- Nutzung sicherer Passwörter
- Nutzung eines Passwortmanagers
- Zwei-Faktor-Authentifizierung für zentrale Accounts, soweit verfügbar
- keine unnötige Weitergabe von Zugangsdaten
- Vertraulichkeitsverpflichtung für einbezogene Personen
- projektbezogene Beschränkung von Zugriffsrechten
- Entzug von Zugängen nach Projektende oder Wegfall der Berechtigung

3. Integrität

L.O.O.P. trifft angemessene Maßnahmen, um personenbezogene Daten vor unbefugter Veränderung, Manipulation oder unbeabsichtigter Veränderung zu schützen.

Maßnahmen können insbesondere sein:

- Zugriffsrechte nur für berechtigte Personen
- Änderungen an Systemen nur durch befugte Personen
- Dokumentation wesentlicher Änderungen nach technischer und organisatorischer Möglichkeit
- Trennung von Entwicklungs-, Test- und Produktivbereichen, soweit angemessen
- Prüfung von Änderungen vor produktiver Nutzung, soweit projektbezogen erforderlich
- Versionierung oder Änderungsdokumentation nach technischer Möglichkeit

- Freigabeprozesse für produktive Aktivierungen

4. Verfügbarkeit und Belastbarkeit

L.O.O.P. trifft angemessene Maßnahmen, um die Verfügbarkeit und Belastbarkeit der eingesetzten Systeme im Rahmen der vereinbarten Leistungen zu unterstützen.

Maßnahmen können insbesondere sein:

- Hosting bei geeigneten Anbietern
- Einsatz eigener Server oder projektbezogener Hostinglösungen
- regelmäßige Backups
- Backup-Rotation bis zu 30 Tage, soweit nicht anders vereinbart
- technische Wiederherstellung im Rahmen der vorhandenen Backups
- Wartung und Sicherheitsupdates nach technischer Erforderlichkeit
- Überwachung zentraler Systeme nach Maßgabe des jeweiligen Servicepakets
- technische Begrenzung von Zugriffsrechten
- Schutz vor unbefugten Zugriffen
- Berücksichtigung von Drittanbieter-Limits und API-Beschränkungen

Eine bestimmte Verfügbarkeit wird nur geschuldet, wenn sie ausdrücklich als SLA oder Service Level Agreement vereinbart ist.

5. Wiederherstellbarkeit

Backups dienen der technischen Sicherheit, Systemstabilität und Wiederherstellung bei technischen Störungen.

Maßnahmen können insbesondere sein:

- regelmäßige Sicherungen relevanter Systeme, soweit technisch und projektbezogen vorgesehen
- Wiederherstellung aus Backups im Rahmen der technischen Möglichkeiten
- Backup-Rotation bis zu 30 Tage, soweit nicht anders vereinbart
- getrennte Behandlung von Backups und regulären Datenexporten
- Nutzung von Backups grundsätzlich nur im Wiederherstellungsfall

Backups sind nicht Bestandteil eines regulären Datenexports.

6. Zugriffskontrolle

L.O.O.P. schützt Systeme, Zugänge und technische Zugangsmittel vor unberechtigter Nutzung.

Maßnahmen können insbesondere sein:

- individuelle Benutzerkonten, soweit technisch möglich
- Adminzugänge nur für berechtigte Personen
- sichere Passwortvergabe
- Zwei-Faktor-Authentifizierung, soweit verfügbar
- regelmäßige Prüfung von Zugriffsrechten

- Sperrung oder Entzug nicht mehr benötigter Zugänge
- Behandlung von API-Keys, Token und Webhook-URLs wie Passwörter
- keine ungesicherte Speicherung sensibler Zugangsmittel in frei zugänglichen Dokumenten

7. Übertragungskontrolle

L.O.O.P. trifft angemessene Maßnahmen, um personenbezogene Daten bei Übertragung oder Weitergabe zu schützen.

Maßnahmen können insbesondere sein:

- verschlüsselte Übertragung über HTTPS/TLS, soweit technisch möglich
- datenminimierte Weitergabe an Drittanbieter
- keine unnötige Übermittlung besonderer Kategorien personenbezogener Daten
- sichere Übermittlung von Zugangsdaten und API-Keys
- projektbezogene Prüfung eingesetzter Schnittstellen
- Beschränkung von Datenflüssen auf den vereinbarten Zweck

8. Eingabe- und Änderungskontrolle

L.O.O.P. wirkt darauf hin, dass wesentliche Eingaben, Änderungen und Verarbeitungsvorgänge im Rahmen der eingesetzten Systeme nachvollziehbar bleiben, soweit dies technisch und wirtschaftlich angemessen ist.

Maßnahmen können insbesondere sein:

- Protokollierung nach Systemfunktionalität
- Dokumentation wesentlicher Projektentscheidungen
- Freigaben per E-Mail, Projektmanagementsystem oder sonstiger Textform
- Nachvollziehbarkeit technischer Änderungen nach Möglichkeit
- Eingrenzung von Adminrechten
- Dokumentation relevanter Weisungen des Auftraggebers

9. Auftragskontrolle

L.O.O.P. verarbeitet personenbezogene Daten des Auftraggebers nur im Rahmen des jeweiligen Auftrags und nach dokumentierter Weisung des Auftraggebers.

Maßnahmen können insbesondere sein:

- AVV mit dem Auftraggeber
- projektbezogene Beschreibung der Verarbeitung
- vertragliche Verpflichtung von Unterauftragsverarbeitern, soweit erforderlich
- Dokumentation eingesetzter Systeme und Anbieter
- Verarbeitung nur für vereinbarte Zwecke
- keine Nutzung von Kundendaten für eigene Zwecke, soweit nicht gesetzlich erlaubt oder vertraglich vereinbart

10. Trennungskontrolle

L.O.O.P. trifft angemessene Maßnahmen zur Trennung von Kundendaten, Projektdaten und Systembereichen, soweit dies technisch möglich und projektbezogen erforderlich ist.

Maßnahmen können insbesondere sein:

- getrennte Workspaces
- getrennte Projekte
- getrennte Datenbanken oder Tabellen
- rollenbasierte Zugriffe
- separate Instanzen oder Server, soweit vereinbart
- logische Trennung innerhalb eingesetzter Tools
- Zugriffsbeschränkung auf projektbezogene Daten

11. Datenminimierung und datenschutzfreundliche Voreinstellungen

L.O.O.P. wirkt auf eine datenminimierte Verarbeitung hin.

Maßnahmen können insbesondere sein:

- Verarbeitung nur erforderlicher Daten
- Beschränkung von Datenflüssen auf den Projektzweck
- Hinweise an Kunden zur Vermeidung sensibler Daten
- keine Verarbeitung besonderer Kategorien personenbezogener Daten ohne ausdrückliche Vereinbarung
- Pseudonymisierung oder Anonymisierung, soweit technisch sinnvoll und projektbezogen möglich
- Reduzierung gespeicherter Kommunikationsinhalte, soweit möglich
- Beschränkung von Logs und Protokollen auf erforderliche Zwecke

12. Prüfung, Bewertung und Verbesserung

L.O.O.P. überprüft die eingesetzten technischen und organisatorischen Maßnahmen regelmäßig und anlassbezogen.

Anlässe können insbesondere sein:

- neue Projekte
- neue Tools
- neue Unterauftragsverarbeiter
- Sicherheitsvorfälle
- wesentliche technische Änderungen
- geänderte rechtliche Anforderungen
- geänderte Kundenanforderungen

13. Unterauftragsverarbeiterliste

Die folgende Liste enthält typische Unterauftragsverarbeiter, Anbieter und technische Dienstleister, die je nach Projekt eingesetzt werden können. Nicht jeder Anbieter wird automatisch in jedem Projekt eingesetzt. Maßgeblich ist der tatsächliche projektbezogene Einsatz.

13.1 ALL-INKL.COM

Anbieter: ALL-INKL.COM / Neue Medien Münnich

Sitz: Deutschland

Zweck: Website-Hosting, technische Bereitstellung, ggf. E-Mail- oder Serverleistungen

Datenkategorien: technische Daten, Website-Daten, Kommunikationsdaten, soweit eingesetzt

Drittlandtransfer: grundsätzlich nein, soweit Verarbeitung in Deutschland/EU erfolgt

Status: soweit eingesetzt

13.2 Hetzner

Anbieter: Hetzner Online GmbH

Sitz: Deutschland

Zweck: Serverhosting, Automationsserver, technische Infrastruktur

Datenkategorien: Projekt- und Systemdaten, technische Daten, Kommunikations- und Kundendaten je nach Projekt

Drittlandtransfer: grundsätzlich nein, soweit Verarbeitung in Deutschland/EU erfolgt

Status: soweit eingesetzt

13.3 n8n

Anbieter: n8n, je nach Projekt selbst gehostet oder Anbieterleistung

Sitz: projektabhängig

Zweck: Automationsplattform, Workflows, Schnittstellen, Datenübertragung

Datenkategorien: Daten aus angebundenen Systemen, Kommunikationsdaten, CRM-Daten, technische Daten

Drittlandtransfer: abhängig von Hosting-Variante und Projekt

Status: soweit eingesetzt

13.4 OpenAI

Anbieter: OpenAI

Sitz / Verarbeitung: projekt- und dienstabhängig

Zweck: KI-Antwortgenerierung, Sprachmodell, Klassifizierung, Zusammenfassung, Assistenzfunktionen

Datenkategorien: Prompts, Kommunikationsinhalte, Kontextdaten, Systemanweisungen, Ergebnisdaten

Drittlandtransfer: möglich

Transfergrundlage / Schutzmaßnahmen: abhängig von Anbieterbedingungen, Accounttyp, Einstellungen, Angemessenheitsbeschluss, EU-US Data Privacy Framework, Standardvertragsklauseln oder sonstigen geeigneten Garantien

Minimierungsmaßnahmen: Datenminimierung, Pseudonymisierung/Anonymisierung soweit möglich, keine besonderen Kategorien personenbezogener Daten ohne Sondervereinbarung. Empfohlene Konfiguration, soweit verfügbar und projektbezogen angemessen: Business-, Enterprise- oder API-Account mit deaktivierter

Trainingsnutzung, store=false, Zero Data Retention oder vergleichbaren Datenkontroll- und Minimierungseinstellungen.

Hinweis: Eine Zero-Data-Retention- oder Nicht-Speicherungs-Konfiguration gilt nur, sofern sie verfügbar, genehmigt, technisch aktiviert und vertraglich vereinbart ist. Eine pauschale Nicht-Speicherungszusage wird nicht abgegeben.

Status: soweit eingesetzt

13.5 Anthropic / Claude

Anbieter: Anthropic

Sitz / Verarbeitung: projekt- und dienstabhängig

Zweck: KI-Antwortgenerierung, Sprachmodell, Analyse, Zusammenfassung, Assistenzfunktionen

Datenkategorien: Prompts, Kommunikationsinhalte, Kontextdaten, Systemanweisungen, Ergebnisdaten

Drittlandtransfer: möglich

Transfergrundlage / Schutzmaßnahmen: abhängig von Anbieterbedingungen, Accounttyp, Einstellungen, Standardvertragsklauseln oder sonstigen geeigneten Garantien

Minimierungsmaßnahmen: Datenminimierung, Pseudonymisierung/Anonymisierung soweit möglich, keine besonderen Kategorien personenbezogener Daten ohne Sondervereinbarung. Empfohlene Konfiguration, soweit verfügbar und projektbezogen angemessen: Business-, Enterprise- oder API-Account mit deaktivierter Trainingsnutzung, Zero Data Retention oder vergleichbaren Datenkontroll- und Minimierungseinstellungen.

Hinweis: Speicherung, Löschung, Protokollierung, Missbrauchsmonitoring und Trainingsnutzung richten sich nach Anbieterbedingungen, Produkt, Accounttyp, Einstellungen und vertraglicher Vereinbarung. Eine pauschale Nicht-Speicherungszusage wird nicht abgegeben.

Status: soweit eingesetzt

13.6 Google

Anbieter: Google Ireland Limited / Google-Unternehmen

Sitz: Irland / USA je nach Dienst

Zweck: Google Calendar, Google Meet, Gmail, Google Workspace, Google Sheets, Terminbuchung, Kommunikation

Datenkategorien: Kontaktdaten, Kalenderdaten, Kommunikationsdaten, technische Daten, Projektinformationen

Drittlandtransfer: möglich

Transfergrundlage / Schutzmaßnahmen: abhängig von Dienst und Einstellungen, Angemessenheitsbeschluss, EU-US Data Privacy Framework, Standardvertragsklauseln oder sonstige Garantien

Status: soweit eingesetzt

13.7 Meta / WhatsApp Cloud API

Anbieter: Meta Platforms Ireland Limited / Meta-Unternehmen

Sitz: Irland / USA je nach Dienst

Zweck: WhatsApp-Kommunikation, WhatsApp Business, Nachrichtenübermittlung

Datenkategorien: Telefonnummern, WhatsApp-Nachrichten, Kommunikationsinhalte, Metadaten

Drittlandtransfer: möglich

Transfergrundlage / Schutzmaßnahmen: abhängig von Dienst, Account und Anbieterbedingungen

Status: soweit eingesetzt

13.8 360dialog

Anbieter: 360dialog GmbH

Sitz: Deutschland

Zweck: WhatsApp Business API Provider, technische Anbindung an WhatsApp

Datenkategorien: Telefonnummern, WhatsApp-Nachrichten, Kommunikationsinhalte, technische Verbindungsdaten

Drittlandtransfer: abhängig von Subdienstleistern und WhatsApp-/Meta-Anbindung

Status: soweit eingesetzt

13.9 Twilio, Vapi, ElevenLabs oder vergleichbare Voice-/Telefonieanbieter

Anbieter: projektabhängig

Sitz / Verarbeitung: projektabhängig

Zweck: Telefonie, Voice Assistant, Sprachverarbeitung, Text-to-Speech, Speech-to-Text, Transkription

Datenkategorien: Telefonnummern, Audiodaten, Gesprächsinhalte, Transkripte, Gesprächszusammenfassungen, technische Daten

Drittlandtransfer: möglich

Transfergrundlage / Schutzmaßnahmen: abhängig von Anbieter, Dienst, Accounttyp und Einstellungen

Status: soweit eingesetzt

13.10 Airtable, Supabase, Google Sheets oder vergleichbare Datenbank-/Tabellenanbieter

Anbieter: projektabhängig

Sitz / Verarbeitung: projektabhängig

Zweck: Datenbanken, Tabellen, strukturierte Speicherung, Projektlogik, Reporting

Datenkategorien: Lead-Daten, CRM-Daten, Projektinformationen, Kommunikationsdaten, technische Daten

Drittlandtransfer: abhängig vom Anbieter

Status: soweit eingesetzt

13.11 HubSpot, Pipedrive, Resmio oder vergleichbare CRM-/Reservierungsanbieter

Anbieter: projektabhängig

Sitz / Verarbeitung: projektabhängig

Zweck: CRM, Kundenverwaltung, Reservierung, Termin- oder Lead-Verwaltung

Datenkategorien: Kontaktdaten, Kundendaten, Kommunikationsdaten, Termin-/Reservierungsdaten, Projektinformationen

Drittlandtransfer: abhängig vom Anbieter

Status: soweit eingesetzt

13.12 WordPress, Elementor und vergleichbare Website-Systeme

Anbieter: projektabhängig

Sitz / Verarbeitung: abhängig von Hosting und Plugins

Zweck: Website-Betrieb, Formulare, Landingpages, technische Funktionen

Datenkategorien: Formular- und Lead-Daten, technische Daten, Website-Daten

Drittlandtransfer: abhängig von Hosting, Plugins und Drittanbietern

Status: soweit eingesetzt

13.13 Make, Zapier oder vergleichbare Automationsdienste

Anbieter: projektabhängig

Sitz / Verarbeitung: projektabhängig

Zweck: Automationen, Schnittstellen, Datenübertragung, Workflows

Datenkategorien: Daten aus angebundenen Systemen, Kommunikationsdaten, CRM-Daten, technische Daten

Drittlandtransfer: möglich

Status: soweit eingesetzt

13.14 Weitere projektbezogene Anbieter

Je nach Projekt können weitere Anbieter eingesetzt werden, wenn dies für die vereinbarte Leistung erforderlich oder zweckmäßig ist. Der konkrete Einsatz ergibt sich aus Angebot, Leistungsbeschreibung, technischer Umsetzung oder projektbezogener Datenschutzanlage.

14. Löschung, Rückgabe, Backups und Drittlandtransfer

14.1 Datenexport und Rückgabe

Soweit technisch möglich und vereinbart, kann der Auftraggeber nach Vertragsende oder auf berechtigte Anfrage einen Export der ihm zugeordneten Kundendaten und Ergebnisdaten erhalten.

Hierzu können insbesondere gehören:

- Leads
- Kontaktdaten
- Formularanfragen
- CRM-Daten
- Buchungen
- Gesprächszusammenfassungen
- Transkripte
- Chatverläufe
- Reports
- Datenbankeinträge
- Performanceergebnisse
- vom Auftraggeber bereitgestellte Inhalte

Der Export erfolgt in einem üblichen, technisch angemessenen Format, zum Beispiel CSV, XLSX, JSON, PDF oder einem vergleichbaren Format, sofern nichts anderes vereinbart ist.

14.2 Nicht vom Export umfasst

Nicht vom Datenexport umfasst sind interne Systemlogik, Promptsysteme, Promptketten, n8n-Workflows, Automationsarchitekturen, Quellcode, Templates, Frameworks, wiederverwendbare Bausteine, interne Methoden,

interne Dokumentationen, Sicherheitskonfigurationen, API-Keys, Zugangsdaten, interne Prüfnotizen und sonstiges Know-how von L.O.O.P., sofern deren Herausgabe nicht ausdrücklich vereinbart wurde.

Eine Herausgabe solcher Bestandteile erfolgt nur bei ausdrücklicher Vereinbarung, insbesondere im Rahmen eines gesondert vergüteten Buyouts oder einer ausdrücklich vereinbarten Systemübergabe.

14.3 Löschung von Kundendaten

Nach Vertragsende löscht oder anonymisiert L.O.O.P. projektbezogene personenbezogene Daten grundsätzlich innerhalb von 30 bis 60 Tagen nach Abschluss eines vereinbarten Exports oder nach Ablauf einer angemessenen Exportfrist, soweit keine gesetzlichen Aufbewahrungspflichten, berechtigten Interessen, Abrechnungszwecke, Nachweispflichten oder abweichenden Vereinbarungen entgegenstehen.

14.4 Backups

Backups dienen der technischen Sicherheit, Wiederherstellung und Systemstabilität. Sie sind nicht Bestandteil des regulären Datenexports.

Gelöschte Daten können noch bis zum Ablauf der jeweiligen Backup-Rotation in Sicherungskopien enthalten sein. Backups werden grundsätzlich nur im Wiederherstellungsfall verwendet und planmäßig überschrieben. Die regelmäßige Backup-Rotation beträgt, soweit nicht anders vereinbart, bis zu 30 Tagen.

14.5 Vertrags-, Abrechnungs- und Nachweisdaten

Vertragsunterlagen, Rechnungsdaten, Zahlungsinformationen, buchhaltungsrelevante Unterlagen, Projektkommunikation und sonstige Nachweisdaten können über das Vertragsende hinaus gespeichert werden, soweit dies zur Erfüllung gesetzlicher Aufbewahrungspflichten, zur Abrechnung, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zur Dokumentation der Leistungserbringung erforderlich ist.

14.6 Drittlandtransfer

Soweit Anbieter mit Sitz oder Verarbeitung außerhalb der EU/des EWR eingesetzt werden, erfolgt eine Übermittlung nur auf Grundlage geeigneter Garantien oder gesetzlicher Grundlagen.

Hierzu können insbesondere gehören:

• Angemessenheitsbeschluss

• EU-US Data Privacy Framework

• Standardvertragsklauseln

• zusätzliche technische und organisatorische Schutzmaßnahmen

• ausdrückliche Einwilligung

• gesetzliche Ausnahmen

Bei KI-Anbietern wie OpenAI, Anthropic Claude oder vergleichbaren Diensten gilt: Speicherung, Protokollierung, Löschung, Missbrauchsmonitoring, Trainingsnutzung und Datenkontrollen richten sich nach dem jeweils eingesetzten Produkt, Accounttyp, Endpoint, den Einstellungen und den Anbieterbedingungen. Eine Zero-Data-Retention-Konfiguration, store=false oder vergleichbare Nicht-Speicherungs- bzw. Minimierungseinstellung gilt nur, sofern sie verfügbar, genehmigt, technisch aktiviert und vertraglich vereinbart ist.

Änderungsvermerk

Version 1.1 enthält insbesondere einen stärkeren Querverweis zum AVV, zu AGB und SLA sowie präzisierte Hinweise zu OpenAI, Anthropic Claude, Drittlandtransfers, Zero Data Retention, store=false und vergleichbaren Datenkontroll- und Minimierungseinstellungen.