OPEXGUARD

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Muster mit Anlagen: Gegenstand der Verarbeitung, technische und organisatorische Maßnahmen, Unterauftragsverarbeiter, Löschkonzept.

OpexGuard GbR · Muster, Version 0.1 · Stand 24.09.2026 · info@opexguard.de
Die aktuelle Fassung mit allen Anlagen steht unter www.opexguard.de/sicherheit/avv.

Entwurf – die juristische Prüfung steht aus. Mit dem ersten Kundenvertrag wird die geprüfte Fassung veröffentlicht.

INHALT

Die technischen Mechanismen hinter den Zusagen – Hash-Kette, Row-Level Security, Verschlüsselung, Sicherung, Standorte, Datenflüsse – beschreibt die Dokumentation unter **www.opexguard.de/technik**; sie gilt als Teil der Anlage 2.

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

[Name des Auftraggebers], [Anschrift], vertreten durch [Vertretungsberechtigte] – nachfolgend **Auftraggeber** (Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO) –

und

OpexGuard GbR, Pommernstr. 12, 67454 Haßloch, vertreten durch die Gesellschafter Alexander Axt und Boris Nicolai – nachfolgend **Auftragnehmer** (Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO) –

§ 1 Gegenstand und Dauer

1. Der Auftragnehmer betreibt für den Auftraggeber die Plattform OpexGuard zur Überwachung von Sendungen, zur Bearbeitung von Vorgängen und Reklamationen gegenüber Carriern und zur Verwaltung von Belegen (nachfolgend **Plattform**). Grundlage ist der zwischen den Parteien geschlossene Vertrag über die Nutzung der Plattform vom [Datum] (nachfolgend **Hauptvertrag**). Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers.
2. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus Art. 28 DSGVO. Er gilt für alle Tätigkeiten, bei denen der Auftragnehmer oder seine Unterauftragsverarbeiter mit personenbezogenen Daten des Auftraggebers in Berührung kommen.
3. Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrags. Er endet, wenn der Hauptvertrag endet und der Auftragnehmer die Daten nach § 10 zurückgegeben und gelöscht hat.

§ 2 Art und Zweck der Verarbeitung, Datenkategorien, betroffene Personen

1. Gegenstand, Art und Zweck der Verarbeitung, die Kategorien personenbezogener Daten und die Kategorien betroffener Personen sind in **Anlage 1** beschrieben.
2. Die Verarbeitung findet ausschließlich in Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums statt. Eine Verarbeitung in einem Drittland ist nur durch die in **Anlage 3** genannten Unterauftragsverarbeiter und nur unter den Voraussetzungen der Art. 44 ff. DSGVO zulässig (§ 11).

§ 3 Weisungen des Auftraggebers

1. Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers. Die Weisungen sind mit diesem Vertrag, dem Hauptvertrag und den Anlagen erteilt; sie umfassen die Nutzung der Funktionen der Plattform durch die Benutzer des Auftraggebers und die in Anlage 1 beschriebenen automatisierten Abläufe.
2. Der Auftraggeber kann Weisungen jederzeit ändern, ergänzen oder ersetzen. Weisungen erfolgen in Textform (E-Mail genügt) an die in § 13 genannte Kontaktadresse des Auftragnehmers; mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.
3. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.
4. Geht eine Weisung über den im Hauptvertrag vereinbarten Leistungsumfang hinaus, können die Parteien eine Vergütung des Mehraufwands vereinbaren.

§ 4 Pflichten des Auftragnehmers

1. **Vertraulichkeit.** Der Auftragnehmer stellt sicher, dass alle Personen, die personenbezogene Daten des Auftraggebers verarbeiten können, zur Vertraulichkeit verpflichtet sind (Art. 28 Abs. 3 lit. b DSGVO). Das sind heute die beiden Gesellschafter des Auftragnehmers; sie haben sich schriftlich verpflichtet. Die Verpflichtung besteht nach Ende der Tätigkeit fort.
2. **Sicherheit der Verarbeitung.** Der Auftragnehmer trifft die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält sie für die Dauer des Vertrags aufrecht. Er darf sie weiterentwickeln, solange das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen dokumentiert er und stellt die aktuelle Fassung der Anlage 2 unter www.opexguard.de/sicherheit/avv bereit.
3. **Kein eigener Zweck.** Der Auftragnehmer nutzt die Daten des Auftraggebers ausschließlich zur Erbringung der Leistungen aus dem Hauptvertrag – nicht für eigene Zwecke, nicht für Zwecke Dritter, nicht zur Anreicherung anderer Datenbestände und nicht zum Training von Modellen.
4. **Verzeichnis und Nachweise.** Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dem Auftraggeber die für dessen Nachweispflichten erforderlichen Informationen zur Verfügung (§ 9).
5. **Ansprechpartner.** Ansprechpartner des Auftragnehmers für Datenschutzfragen ist die Geschäftsführung (§ 13). Ein Datenschutzbeauftragter ist nach Art. 37 DSGVO und § 38 BDSG nicht zu benennen; ändert sich das, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten unaufgefordert mit.
6. **Unterstützung.** Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Pflichten aus Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen (§§ 6 bis 8).
7. **Kontrolle durch Behörden.** Wird der Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung von einer Aufsichtsbehörde geprüft oder erhält er ein behördliches Auskunftsverlangen, das Daten des Auftraggebers betrifft, informiert er den Auftraggeber unverzüglich, soweit das rechtlich zulässig ist.

§ 5 Unterauftragsverarbeiter

1. Der Auftraggeber genehmigt die in **Anlage 3** genannten Unterauftragsverarbeiter mit Abschluss dieses Vertrags (allgemeine Genehmigung nach Art. 28 Abs. 2 DSGVO).
2. Der Auftragnehmer darf weitere Unterauftragsverarbeiter hinzuziehen oder bestehende ersetzen. Er informiert den Auftraggeber vorab in Textform an die in § 13 genannte Kontaktadresse und veröffentlicht die aktualisierte Liste unter www.opexguard.de/sicherheit/avv – mindestens **30 Tage** bevor der neue Unterauftragsverarbeiter Daten des Auftraggebers verarbeitet. Die Mitteilung nennt Name, Sitz, Leistung, Ort der Verarbeitung und, bei Drittlandbezug, die Übermittlungsgrundlage.
3. Der Auftraggeber kann der Änderung innerhalb der Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Kommt keine Einigung zustande, kann jede Partei den Hauptvertrag mit einer Frist von 30 Tagen zum Monatsende kündigen; bis dahin setzt der Auftragnehmer den betroffenen Unterauftragsverarbeiter für den Auftraggeber nicht ein, soweit das technisch möglich ist.
4. Der Auftragnehmer legt jedem Unterauftragsverarbeiter dieselben Datenschutzpflichten auf, die in diesem Vertrag vereinbart sind, insbesondere hinreichende Garantien für technische und organisatorische Maßnahmen. Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Pflichterfüllung.

5. Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind Stellen, die der Auftraggeber selbst beauftragt hat oder die als eigenständig Verantwortliche handeln – insbesondere die Carrier, mit denen der Auftragnehmer im Auftrag des Auftraggebers zu einzelnen Sendungen kommuniziert (Nachforschungen, Reklamationen, Belege), sowie der Identitätsanbieter des Auftraggebers (Microsoft Entra ID des Auftraggebers), über den sich dessen Benutzer anmelden.

§ 6 Rechte der betroffenen Personen

1. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anfragen betroffener Personen nach Art. 12 bis 22 DSGVO zu beantworten. Die Plattform stellt dafür bereit: Suche und Export der zu einer Person gespeicherten Daten, Berichtigung durch die Benutzer des Auftraggebers, Anonymisierung von Benutzerdaten (unumkehrbar) sowie die in Anlage 4 beschriebenen Lösch- und Anonymisierungsabläufe.
2. Wendet sich eine betroffene Person – zum Beispiel der Empfänger einer Sendung – direkt an den Auftragnehmer, beantwortet dieser die Anfrage nicht in der Sache, sondern leitet sie **innerhalb von zwei Werktagen** an die in § 13 genannte Kontaktadresse des Auftraggebers weiter und informiert die betroffene Person, dass der Auftraggeber Verantwortlicher ist.
3. Der Auftragnehmer gibt ohne Weisung des Auftraggebers keine Auskunft an Dritte über die im Auftrag verarbeiteten Daten.

§ 7 Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten des Auftraggebers (Art. 4 Nr. 12 DSGVO) **unverzüglich, spätestens 24 Stunden** nachdem er von ihr Kenntnis erlangt hat, an die in § 13 genannte Kontaktadresse.
2. Die Meldung enthält, soweit bekannt, die in Art. 33 Abs. 3 DSGVO genannten Angaben: Art der Verletzung, betroffene Datenkategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen sowie einen Ansprechpartner. Informationen, die noch nicht vorliegen, reicht der Auftragnehmer ohne unangemessene Verzögerung nach.
3. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO und dokumentiert Verletzungen samt Ursachen, Auswirkungen und Abhilfemaßnahmen. Er trifft unverzüglich die Maßnahmen, die zur Sicherung der Daten und zur Minderung nachteiliger Folgen erforderlich sind.
4. Die Meldepflicht besteht unabhängig davon, ob die Verletzung beim Auftragnehmer oder bei einem seiner Unterauftragsverarbeiter eingetreten ist.

§ 8 Datenschutz-Folgenabschätzung und vorherige Konsultation

Der Auftragnehmer unterstützt den Auftraggeber bei einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und bei einer vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DSGVO), soweit sie die Verarbeitung auf der Plattform betreffen – insbesondere mit der technischen Dokumentation unter www.opexguard.de/technik, der Beschreibung der Datenflüsse und den Anlagen dieses Vertrags.

§ 9 Kontrollrechte des Auftraggebers

1. Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind. Dazu gehören: die technische

Dokumentation der Plattform, die jeweils aktuellen Anlagen dieses Vertrags, das Verzeichnis nach Art. 30 Abs. 2 DSGVO, Exporte des Änderungsprotokolls des Auftraggebers und die Ergebnisse eigener oder externer Prüfungen, soweit vorhanden.

2. Dem Auftraggeber oder einem von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer richtet der Auftragnehmer auf Wunsch eine reine Leserolle auf dem Mandanten des Auftraggebers ein, mit der sich Sendungen, Dokumente und das Änderungsprotokoll einsehen lassen.
3. Der Auftraggeber kann darüber hinaus einmal je Vertragsjahr sowie bei konkretem Anlass eine Überprüfung – einschließlich Inspektionen – durchführen oder durchführen lassen. Er kündigt sie mindestens **14 Tage** vorher an; die Parteien stimmen Umfang, Zeit und Form ab. Prüfungen finden vorrangig aus der Ferne (Dokumente, Bildschirmfreigabe, Leserolle) statt; einen Betriebsstandort im Sinne eines Rechenzentrums unterhält der Auftragnehmer nicht, die Infrastruktur wird von den in Anlage 3 genannten Unterauftragsverarbeitern betrieben, deren Zertifizierungen und Prüfberichte (ISO 27001, SOC 1/2/3) der Auftragnehmer benennt.
4. Übersteigt der Aufwand einer Prüfung beim Auftragnehmer einen Personentag, vereinbaren die Parteien vorab eine angemessene Erstattung, es sei denn, die Prüfung deckt einen Verstoß des Auftragnehmers auf.

§ 10 Löschung und Rückgabe nach Vertragsende

1. Während der Vertragslaufzeit löscht oder anonymisiert der Auftragnehmer personenbezogene Daten nach den in **Anlage 4** vereinbarten Fristen.
2. Nach Beendigung des Hauptvertrags stellt der Auftragnehmer dem Auftraggeber alle im Auftrag verarbeiteten Daten für **30 Tage** zum Abruf bereit: jede Liste der Plattform als CSV, jedes Dokument mit allen Versionen, das Änderungsprotokoll als JSON. Auf Wunsch übergibt der Auftragnehmer die Daten stattdessen auf einem vereinbarten Weg.
3. Nach Ablauf der 30 Tage – oder früher, wenn der Auftraggeber die Übergabe in Textform bestätigt – löscht der Auftragnehmer alle Daten des Auftraggebers einschließlich Kopien, soweit nicht eine gesetzliche Aufbewahrungspflicht des Auftragnehmers entgegensteht; in diesem Fall schränkt er die Verarbeitung auf die Aufbewahrung ein. Daten in Sicherungskopien werden mit deren Rotation gelöscht (spätestens 14 Tage nach der Löschung in der Datenbank). Den Vollzug bestätigt der Auftragnehmer dem Auftraggeber in Textform.
4. Die Regelung zum Archiv des Änderungsprotokolls in Anlage 4 bleibt unberührt.

§ 11 Verarbeitung in Drittländern

Der Auftragnehmer verarbeitet Daten des Auftraggebers ausschließlich in der Europäischen Union. Soweit ein in Anlage 3 genannter Unterauftragsverarbeiter Daten in einem Drittland verarbeitet oder von dort auf sie zugreift, geschieht das nur auf einer Grundlage nach Art. 44 ff. DSGVO – Angemessenheitsbeschluss (einschließlich EU-US Data Privacy Framework) oder Standardvertragsklauseln der Europäischen Kommission mit ergänzenden Maßnahmen –, die in Anlage 3 je Unterauftragsverarbeiter benannt ist.

§ 12 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO und den Regelungen des Hauptvertrags. Eine Haftungsbeschränkung im Hauptvertrag gilt nicht für Ansprüche betroffener Personen nach Art. 82 DSGVO.

§ 13 Kontaktadressen, Schlussbestimmungen

1. Kontaktadresse des Auftragnehmers für Weisungen, Meldungen und Anfragen: OpexGuard GbR, info@opexguard.de, Telefon 0172 3827750. Kontaktadresse des Auftraggebers: [Name, Funktion, E-Mail, Telefon].
2. Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor, soweit sie den Schutz personenbezogener Daten betreffen.
3. Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt; an die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.
4. Es gilt das Recht der Bundesrepublik Deutschland.

Anlagen: **1** Gegenstand der Verarbeitung · **2** Technische und organisatorische Maßnahmen · **3** Unterauftragsverarbeiter · **4** Löschkonzept und Fristen

[Ort, Datum] · für den Auftraggeber: _____ · für den Auftragnehmer: _____

Anlage 1 – Gegenstand der Verarbeitung

1. Gegenstand und Zweck

Der Auftragnehmer stellt dem Auftraggeber die Plattform OpexGuard als Software-as-a-Service bereit und betreibt sie. Der Auftraggeber nutzt sie, um Sendungen zu überwachen, Abweichungen zu erkennen, Vorgänge und Reklamationen gegenüber Carriern zu führen, Ablieferbelege und weitere Dokumente je Sendung zu verwalten und Fristen im Blick zu behalten. Zweck der Verarbeitung ist ausschließlich die Bearbeitung dieser Vorgänge des Auftraggebers.

2. Art der Verarbeitung

Erheben (Import, Schnittstellen, Eingabe durch Benutzer), Speichern, Ordnen, Anpassen, Abfragen, Verwenden, Übermitteln an die in Anlage 3 genannten Unterauftragsverarbeiter und – im Auftrag des Auftraggebers – an Carrier, Archivieren, Anonymisieren und Löschen. Es findet keine automatisierte Entscheidung im Einzelfall und kein Profiling im Sinne von Art. 22 DSGVO statt.

3. Kategorien personenbezogener Daten

KATEGORIE	INHALT
Sendungsdaten	Sendungs- und Tracking-Nummer, Carrier, Service, Status, Gewicht, Maße, Zeiten; Absender und Empfänger: Name, Firma, Straße, Ort, Postleitzahl, Land, E-Mail-Adresse, Telefonnummer
Tracking-Ereignisse	Status, Ort und Zeitpunkt je Ereignis, vom Carrier bzw. Tracking-Dienstleister
Vorgänge und Reklamationen	Freitexte, Beträge, Fristen, Zuordnung zu Sendungen, Bearbeiter
Dokumente	Ablieferbelege, Frachtbriefe, Rechnungen, Zollpapiere, Fotos – als Datei; darin häufig Namen, Anschriften, Unterschriften
E-Mails	Kopfzeilen, Text und Anhänge der Carrier-Kommunikation, die der Auftraggeber weiterleitet oder über eine Postfach-Anbindung einliefert
Benutzerdaten	Name, E-Mail-Adresse, Objekt- und Verzeichniskennung aus Microsoft Entra ID, Rollen, Einladungen
Änderungsprotokoll	Benutzerkennung, Rolle, Zeitpunkt, Objekt und alte/neue Werte jeder Änderung an fachlichen Daten
Telemetrie	technische Kennzahlen, Fehler und Aufrufketten; Benutzerkennungen können in Fehlermeldungen enthalten sein

Zugangsdaten (API-Schlüssel, Carrier-Zugangsdaten, SFTP-Zugänge) werden ausschließlich als Hash bzw. verschlüsselt gespeichert und sind keine personenbezogenen Daten im Sinne dieser Anlage. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung; der Auftraggeber stellt sicher, dass er solche Daten nicht in Freitexte oder Dokumente einbringt.

4. Kategorien betroffener Personen

- Empfänger und Absender von Sendungen des Auftraggebers – Privatpersonen und Ansprechpartner bei Unternehmen
- Mitarbeiter des Auftraggebers, die die Plattform nutzen (Benutzer)
- Ansprechpartner bei Carriern und anderen Beteiligten, deren Daten in Vorgängen, E-Mails oder Dokumenten enthalten sind

5. Automatisierte Abläufe als Weisung

Mit diesem Vertrag weist der Auftraggeber den Auftragnehmer an, folgende Abläufe automatisiert auszuführen, soweit der Auftraggeber sie in der Plattform aktiviert oder nutzt:

1. **Tracking:** Übermittlung von Tracking-Nummer und Carrier je Sendung an den Tracking-Dienstleister (Anlage 3) und Abruf der Ereignisse.
2. **Versandlabels:** Übermittlung von Absender- und Empfängeradresse an den Tracking-/Label-Dienstleister zur Erzeugung eines Labels, wenn der Auftraggeber die Funktion nutzt.
3. **Import:** Übernahme von Sendungsdaten per CSV, Schnittstelle oder SFTP-Abruf aus Systemen des Auftraggebers.
4. **Postfach-Abruf:** Abruf und Zuordnung von Carrier-E-Mails aus einem vom Auftraggeber bestimmten Postfach, sobald die Funktion für den Auftraggeber eingerichtet ist.
5. **Änderungsprotokoll:** Protokollierung jeder Änderung an fachlichen Daten und Archivierung des Protokolls nach 90 Tagen.
6. **Aufbewahrung und Löschung:** Anonymisierung und Löschung nach den Fristen in Anlage 4.

6. Ort der Verarbeitung

Datenbank, Anwendung, Dokumentenspeicher, Archiv und Telemetrie laufen in Rechenzentren von Microsoft Azure in der Region **Schweden-Mitte** (EU). Die Oberfläche der Plattform (statische Dateien ohne Kundendaten) wird über ein Content Delivery Network ausgeliefert. Ausnahmen mit Drittlandbezug sind in Anlage 3 je Unterauftragsverarbeiter genannt.

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

Die Maßnahmen beschreiben den Stand der Plattform und des Betriebs. Was erst mit dem Produktivstart hinzukommt, ist so gekennzeichnet. Die technischen Mechanismen sind in der Dokumentation unter www.opexguard.de/technik im Einzelnen beschrieben; sie gilt als Teil dieser Anlage.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

- Der Auftragnehmer betreibt keine eigenen Rechenzentren oder Serverräume. Alle Systeme laufen in Rechenzentren von Microsoft Azure (Region Schweden-Mitte); für den physischen Zutritt gelten die Maßnahmen von Microsoft (Zutrittskontrolle, Videoüberwachung, Sicherheitspersonal, Besucherregelung), nachgewiesen durch ISO/IEC 27001 und SOC 1/2/3 (Berichte im Microsoft Service Trust Portal).
- Die Arbeitsplätze der beiden Gesellschafter befinden sich in deren Privaträumen. Dritte haben keinen Zugriff auf die Arbeitsgeräte; Geräte werden bei Abwesenheit gesperrt und in Abwesenheit verschlossen aufbewahrt.

1.2 Zugangskontrolle

- Anmeldung von Personen an der Plattform ausschließlich über Microsoft Entra ID (OpenID Connect) mit dem Konto des jeweiligen Unternehmens; Multi-Faktor-Authentifizierung, Kennwortregeln und Sperrung beim Ausscheiden steuert der Auftraggeber in seinem Verzeichnis. Nur Verzeichnisse, die der Auftragnehmer je Kunde freigegeben hat, werden akzeptiert.
- Systemzugänge (Schnittstelle) nur über API-Schlüssel je Mandant und Rolle, gespeichert ausschließlich als SHA-256-Hash, widerrufbar, ratenbegrenzt.
- Administrative Zugänge des Auftragnehmers (Azure, Microsoft 365, Azure DevOps) sind auf die beiden Gesellschafter beschränkt und durch Multi-Faktor-Authentifizierung geschützt. Es gibt keine geteilten Konten.
- Dienste greifen untereinander ausschließlich über verwaltete Identitäten (Managed Identity) zu; es gibt keine Verbindungszeichenfolgen und keine Kontoschlüssel in Code oder Konfiguration. Geheimnisse liegen ausschließlich im Azure Key Vault (Löschschutz aktiv).
- Setup- und Betreiber-Schlüssel sind gedrosselt, jeder Gebrauch wird protokolliert.
- Arbeitsgeräte der Gesellschafter: vollständige Festplattenverschlüsselung, automatische Bildschirmsperre, aktuelle Sicherheitsupdates, Passwortmanager. Kundendaten werden nicht dauerhaft auf Arbeitsgeräten gespeichert; zur Fehleranalyse heruntergeladene Daten werden nach Abschluss gelöscht.

1.3 Zugriffskontrolle

- Rollen- und Rechtekonzept: Rechte werden je Rolle vergeben (Systemrollen Mandanten-Administrator, Mitglied, Prüfer, Integration; weitere Rollen je Kunde), die Anwendung prüft jedes Recht serverseitig. Der Auftraggeber verwaltet die Rollen seiner Benutzer selbst.
- Betreiberzugriff nur mit benannten Identitäten der beiden Gesellschafter; jeder Zugriff auf Kundendaten erfolgt über die protokollierte Anwendung. Eine Auslieferung in die Produktivumgebung verlangt eine Freigabe durch einen Menschen.

- Prüfern des Auftraggebers steht die Systemrolle „Prüfer“ zur Verfügung: ausschließlich lesender Zugriff, einschließlich Export des Änderungsprotokolls, Integritätsprüfung und Prüfpaket je Sendung.

1.4 Trennungskontrolle

- Mandantentrennung auf Datenbankebene: Row-Level-Security in PostgreSQL auf jedem Lese- und Schreibpfad mit einer eigenen Datenbankrolle der Anwendung. Beim Start prüft die Anwendung die Trennung mit einem Selbsttest und bricht bei Fehlschlag ab.
- Getrennte Umgebungen für Entwicklung, Test und Produktion mit jeweils eigener Infrastruktur; Produktivdaten werden nicht in andere Umgebungen kopiert.
- Dokumentenspeicher und Archiv des Änderungsprotokolls sind getrennte Speicherkonten ohne öffentlichen Zugriff.

1.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Transport ausschließlich über HTTPS mit TLS 1.2 oder höher – zwischen Browser und Plattform, zwischen den Diensten und zu Unterauftragsverarbeitern.
- Speicherung: Datenbank, Dokumentenspeicher, Archiv und Sicherungen sind bei Microsoft Azure im Ruhezustand verschlüsselt (AES-256, von Microsoft verwaltete Schlüssel).
- Zugangsdaten zu Carriern werden zusätzlich auf Anwendungsebene mit AES-256 verschlüsselt; der Schlüssel liegt im Azure Key Vault. SFTP-Passwörter werden mit AES-256-GCM verschlüsselt, API-Schlüssel und Einladungscodes nur als Hash gespeichert.
- Benutzerdaten können auf Weisung unumkehrbar anonymisiert werden (Art. 17 DSGVO); Empfängerdaten werden nach den Fristen in Anlage 4 anonymisiert.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Daten verlassen die Plattform nur über authentifizierte, verschlüsselte Schnittstellen und nur an die in Anlage 3 genannten Unterauftragsverarbeiter oder – im Auftrag – an Carrier.
- Kein öffentlicher Zugriff auf Speicherkonten; Downloads von Dokumenten nur nach Anmeldung und Rechteprüfung.
- Die Oberfläche lädt keine Inhalte von Fremdanbietern (Content-Security-Policy).

2.2 Eingabekontrolle

- Änderungsprotokoll: Jede Änderung an fachlichen Daten wird mit Benutzer, Rolle, Zeitpunkt, Objekt sowie altem und neuem Wert protokolliert. Die Einträge sind je Mandant über SHA-256 zu einer Kette verbunden; Zugangsgeheimnisse werden nie protokolliert.
- Nach 90 Tagen werden die Einträge in ein eigenes Archiv übertragen (hochladen, zurücklesen, erst dann löschen); wöchentliche Prüfsummen. Für die Produktivumgebung ist eine Unveränderlichkeits-Richtlinie auf dem Archiv vorgesehen (Sperre mit dem Produktivstart).
- Betreiber-Eingriffe über Setup-Endpunkte werden gesondert protokolliert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Datenbank: tägliche automatische Sicherung, Aufbewahrung 14 Tage, Wiederherstellung auf jeden Zeitpunkt innerhalb der Frist.

- Dokumentenspeicher geografisch redundant mit Lesezugriff (RA-GRS), Archiv geografisch redundant (GRS); Soft-Delete auf beiden Speichern.
- Gesundheitsprüfungen der Anwendung mit automatischem Neustart; nach jedem Deployment automatischer Rollback, wenn die Gesundheitsprüfung fehlschlägt.
- Ratenbegrenzung je API-Schlüssel und gesamt; dauerhafte Nachrichtenwarteschlange (Azure Service Bus), damit Verarbeitungsschritte bei Störungen nicht verloren gehen.
- Alarmierung auf Verfügbarkeit, Fehlerquote, Datenbank und Warteschlange mit Benachrichtigung beider Gesellschafter per E-Mail; geplante Wartung wird in der Anwendung angekündigt.
- Die Wiederherstellung wird geübt und dokumentiert; die Übung in der Produktivumgebung erfolgt mit dem Produktivstart.
- Ein Verfügbarkeitsziel, Reaktionszeiten und Wartungsfenster werden im Hauptvertrag vereinbart.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

4.1 Datenschutz-Management

- Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO), Löschkonzept (Anlage 4), Meldeprozess für Verletzungen des Schutzes personenbezogener Daten und Ablauf für Betroffenenanfragen liegen schriftlich vor und werden mindestens jährlich sowie bei wesentlichen Änderungen überprüft.
- Beide Gesellschafter sind schriftlich zur Vertraulichkeit verpflichtet und halten sich über datenschutzrechtliche Anforderungen auf dem Laufenden; ein Datenschutzbeauftragter ist nicht zu benennen (§ 38 BDSG, Art. 37 DSGVO).

4.2 Sichere Entwicklung und Betrieb

- Jede Änderung durchläuft automatisierte Tests; Abhängigkeiten werden bei jedem Build auf bekannte Schwachstellen geprüft (Abbruch bei Fund) und zusätzlich wöchentlich; Architekturtests sichern Grenzen zwischen den Modulen.
- Die Infrastruktur ist vollständig als Code beschrieben und wird daraus aufgebaut; Änderungen sind nachvollziehbar im Versionskontrollsystem.
- Interne Sicherheitsprüfung im August 2026; ein externer Penetrationstest ist für den Produktivbetrieb vorgesehen.
- Schwachstellen können über die security.txt der Website gemeldet werden.

4.3 Umgang mit Vorfällen

- Meldung an den Auftraggeber unverzüglich, spätestens 24 Stunden nach Kenntnis (§ 7 des Vertrags); Dokumentation von Ursache, Auswirkung und Abhilfe.

4.4 Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

- Es werden nur die Daten erhoben, die für die Bearbeitung der Vorgänge nötig sind; Telemetrie wird nach 30 bzw. 90 Tagen gelöscht; Zugangsgeheimnisse werden nie protokolliert; keine Weitergabe an Werbe-, Analyse- oder KI-Dienste Dritter.

4.5 Auftragskontrolle

- Unterauftragsverarbeiter werden nur mit Vereinbarungen nach Art. 28 DSGVO eingesetzt (Anlage 3); ihre Zertifizierungen und Prüfberichte werden vor Einsatz und danach jährlich gesichtet.

Anlage 3 – Unterauftragsverarbeiter

Stand dieser Liste: 22. September 2026. Änderungen teilt der Auftragnehmer nach § 5 des Vertrags mindestens 30 Tage vorher in Textform mit und veröffentlicht die aktuelle Liste unter www.opexguard.de/sicherheit/avv.

1. Microsoft Ireland Operations Limited

One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland

DIENST	LEISTUNG	DATEN	ORT
Azure Database for PostgreSQL (Flexible Server)	Datenbank der Plattform	alle Daten nach Anlage 1	Schweden-Mitte
Azure Blob Storage (Dokumentenspeicher)	Ablage der Dokumente mit Versionen	Dokumente	Schweden-Mitte, geografisch redundant innerhalb der EU
Azure Blob Storage (Archiv)	Archiv des Änderungsprotokolls	Änderungsprotokoll	Schweden-Mitte, geografisch redundant innerhalb der EU
Azure App Service, Azure Container Registry	Betrieb der Anwendung	alle Daten im Durchlauf	Schweden-Mitte
Azure Key Vault	Verwahrung von Schlüsseln und Geheimnissen	keine personenbezogenen Daten	Schweden-Mitte
Azure Service Bus	Nachrichtenwarteschlange zwischen Verarbeitungsschritten	Kennungen, Sendungsdaten im Durchlauf	Schweden-Mitte
Azure Monitor (Log Analytics, Application Insights)	Protokolle, Metriken, Fehleranalyse	Telemetrie, ggf. Benutzerkennungen	Schweden-Mitte
Azure Static Web Apps	Auslieferung der Oberfläche (Programmcode, keine Kundendaten)	Verbindungsdaten des Browsers	Ressource in East US 2, Auslieferung über ein globales Content Delivery Network
Microsoft 365 (Exchange Online, Microsoft Graph)	Postfach des Auftragnehmers für Postfach-Abruf und Benachrichtigungen, Kalender für Fristen	E-Mails und Termine, die die Plattform im Auftrag versendet, abruft oder anlegt	Europäische Union (EU Data Boundary)

Vertragsgrundlage: Microsoft Products and Services Data Protection Addendum (DPA) als Bestandteil der Microsoft-Produktbestimmungen für Azure und Microsoft 365. **Drittlandbezug:** Die Verarbeitung findet in den genannten EU-Regionen statt. Ein Zugriff durch Microsoft aus Drittländern ist auf Betriebs- und Supportfälle beschränkt und durch das DPA abgedeckt: Standardvertragsklauseln der Europäischen

Kommission sowie die Zertifizierung von Microsoft unter dem EU-US Data Privacy Framework. **Nachweise:** ISO/IEC 27001, 27017, 27018, SOC 1/2/3, BSI C5 (Berichte im Microsoft Service Trust Portal).

2. Tracking- und Label-Dienstleister

Für den Abruf von Tracking-Ereignissen bei den Carriern und – wenn der Auftraggeber die Funktion nutzt – für die Erzeugung von Versandlabels setzt der Auftragnehmer einen Tracking-Dienstleister ein. Name, Anschrift, Sitz und Verarbeitungsorte werden dem Auftraggeber mit Abschluss des Vertrags genannt; der Auftragnehmer behandelt die Wahl seines Dienstleisters als Betriebsgeheimnis. Liegt ein Verarbeitungsort außerhalb der EU oder des EWR, erfolgt die Übermittlung nur auf einer Grundlage nach Art. 44 ff. DSGVO (Angemessenheitsbeschluss oder Standardvertragsklauseln der Europäischen Kommission mit ergänzenden Maßnahmen), die in der Mitteilung benannt wird.

LEISTUNG	DATEN
Abruf von Tracking-Ereignissen bei den Carriern	Tracking-Nummer und Carrier je Sendung
Erzeugung von Versandlabels, wenn der Auftraggeber die Funktion nutzt	Absender- und Empfängeradresse, Paketdaten

Vertragsgrundlage: Vereinbarung zur Auftragsverarbeitung mit dem Anbieter (Art. 28 Abs. 4 DSGVO), die dieselben Pflichten weitergibt wie dieser Vertrag.

3. Keine Unterauftragsverarbeiter

- **Carrier** (zum Beispiel DHL, UPS, FedEx, Hermes, DPD, GLS): Sie befördern die Sendungen des Auftraggebers auf Grundlage des Vertrags zwischen Auftraggeber und Carrier und sind eigenständig Verantwortliche. Übermittelt der Auftragnehmer im Auftrag Daten an einen Carrier (Nachforschung, Reklamation, Beleganforderung), geschieht das als Weisung des Auftraggebers; der Carrier wird dadurch nicht Unterauftragsverarbeiter des Auftragnehmers.
- **Microsoft Entra ID des Auftraggebers:** Die Benutzer melden sich mit dem Verzeichnis des Auftraggebers an; dieses Verzeichnis betreibt der Auftraggeber in eigener Verantwortung.
- **Werbe-, Analyse- oder KI-Dienste Dritter** werden nicht eingesetzt.

Anlage 4 – Löschkonzept und Fristen

Grundsatz: Der Auftragnehmer speichert personenbezogene Daten nur so lange, wie es die Bearbeitung der Vorgänge des Auftraggebers oder eine Aufbewahrungspflicht des Auftraggebers erfordert. Anonymisieren heißt: Alle Angaben, die eine Person erkennen lassen, werden unumkehrbar entfernt; die verbleibenden Sach- und Statistikdaten haben keinen Personenbezug mehr. Der Auftraggeber kann jede Frist durch Weisung verkürzen; verlängern kann er sie, wenn er eine Aufbewahrungspflicht oder ein berechtigtes Interesse nennt.

1. Fristen je Datenart

DATENART	AUSLÖSER	FRIST	WAS GESCHIEHT
Sendungsdaten – Absender und Empfänger (Name, Anschrift, E-Mail, Telefon)	Sendung abgeschlossen (zugestellt, retourniert oder vom Auftraggeber geschlossen) und kein offener Vorgang dazu	**180 Tage**	Anonymisierung: Personenbezüge werden entfernt; Sendungsnummer, Carrier, Status, Zeiten, Gewicht, Postleitzahl und Land bleiben als Statistik
Tracking-Ereignisse	mit der Sendung	mit der Sendung	Angaben, die eine Person erkennen lassen (z. B. Name des Annehmenden), werden entfernt; Status, Ort auf Ortsebene und Zeitpunkt bleiben
Vorgänge und Reklamationen	Vorgang abgeschlossen	**180 Tage**	Freitexte, Beteiligte und Anhänge werden gelöscht; Art, Datum, Betrag und Ergebnis bleiben ohne Personenbezug
E-Mails (weitergeleitete oder abgerufene Carrier-Kommunikation)	mit dem zugeordneten Vorgang bzw. der Sendung; nicht zuordenbare E-Mails: Eingang	**180 Tage** nach Abschluss bzw. **90 Tage** nach Eingang	Löschung
Ablieferbelege, Handelsrechnungen, Frachtbriefe	Ende des Kalenderjahres, in dem das Dokument entstanden ist; bei Belegen zu einer Sendung frühestens Ende des Kalenderjahres, in dem sie abgeschlossen wurde	**8 Jahre** (§ 257 Abs. 4 HGB, § 147 Abs. 3 AO)	Löschung aller Versionen; bis dahin nur Archivieren möglich, kein endgültiges Löschen
Zolldokumente, Ursprungszeugnisse	wie vorstehend	**10 Jahre** (§ 147 Abs. 3 AO)	wie vorstehend

DATENART	AUSLÖSER	FRIST	WAS GESCHIEHT
Lieferscheine, Verträge, Versandlabels, Reports, sonstige Dokumente (Fotos, Notizen)	mit der Sendung bzw. dem Vorgang	**keine Standardfrist** – ohne Festlegung des Auftraggebers **180 Tage**	Löschung
Benutzerkonten	Entfernung des Benutzers durch den Mandanten-Administrator	sofort gesperrt; **12 Monate** danach anonymisiert; auf Weisung sofort	Name, E-Mail-Adresse und Verzeichniskennungen werden unumkehrbar durch ein Pseudonym ersetzt, auch in Vorgängen und im Änderungsprotokoll der Datenbank
Änderungsprotokoll (Datenbank)	Eintrag	**90 Tage**	Übertragung in das Archiv, danach Löschung in der Datenbank
Änderungsprotokoll (Archiv)	Übertragung ins Archiv	**7 Jahre**	Unveränderliche Aufbewahrung auf Weisung des Auftraggebers zum Nachweis der Ordnungsmäßigkeit seiner Vorgänge (Art. 17 Abs. 3 lit. b und e DSGVO): Der Archivspeicher trägt eine Unveränderlichkeits-Richtlinie von sieben Jahren je Archivdatei (Sperre mit dem Produktivstart); nach Ablauf wird jede Archivdatei automatisch gelöscht. Die Frist läuft über das Vertragsende hinaus; bei Vertragsende wird das Archiv dem Auftraggeber übergeben (§ 10). Mit dem Produktivstart enthält das Archiv Namen, Anschriften, E-Mail-Adressen und Telefonnummern von Absendern und Empfängern nur noch als Prüfsumme (schlüsselabhängiger Hash je Mandant); im Klartext stehen sie allein in den 90 Tagen in der Datenbank
Telemetrie und technische Protokolle	Eintrag	**30 Tage** (Protokolle) / **90 Tage** (Application Insights)	automatische Löschung durch Ablauf
Sicherungen der Datenbank	Sicherung	**14 Tage**	automatische Löschung durch Rotation; eine gezielte Löschung einzelner Daten in Sicherungen findet nicht statt. Wird eine Sicherung eingespielt, werden die Löschläufe anschließend erneut ausgeführt

Die Fristen für Dokumente richten sich nach den Aufbewahrungspflichten des Auftraggebers; er legt sie je Dokumenttyp fest und ist dafür verantwortlich, dass sie seinen Pflichten entsprechen. Ohne abweichende Festlegung gelten die Standardwerte der Tabelle.

Maßgeblich ist die **Funktion** des Dokuments, nicht seine Bezeichnung: derselbe Frachtbrief ist als Buchungsbeleg acht, als reiner Handelsbrief sechs Jahre aufzubewahren. Die Standardwerte sind Richtwerte und keine Rechtsberatung; wo mehrere Fristen in Betracht kommen, steht der längere Wert.

⚠️ Für **Lieferscheine, Verträge, Versandlabels und Reports** setzt die Plattform bewusst **keine** Standardfrist: dort entscheidet die Verwendung, und beim Vertrag ist der maßgebliche Fristbeginn – das Ende des Vertrags – der Plattform nicht bekannt. **Ohne Festlegung des Auftraggebers werden diese Dokumente mit ihrer Sendung bzw. ihrem Vorgang nach 180 Tagen gelöscht.** Der Auftraggeber legt eine Frist entweder je Dokumenttyp für seinen Mandanten fest oder am einzelnen Dokument; eine gesetzte Frist lässt sich verlängern, nicht verkürzen.

2. Stand der Umsetzung

Die Plattform setzt die Fristen nach Ziffer 1 selbsttätig um. Ein nächtlicher Lauf anonymisiert oder löscht je Mandant und Datenart, was fällig ist: Sendungen, Vorgänge, E-Mails, Dokumente samt aller Versionen und die Daten entfernter Benutzer. Vor Ablauf ihrer Frist lassen sich Dokumente archivieren, aber nicht endgültig löschen. Das Änderungsprotokoll geht nach 90 Tagen ins Archiv; Name, Firma, Straße, Ort, E-Mail-Adresse und Telefonnummer von Absendern und Empfängern stehen dort nur als Prüfsumme. Telemetrie und Sicherungen laufen nach ihren Fristen ab. Jeder Lauf protokolliert, was wann nach welcher Regel entfernt wurde – ohne die entfernten Daten selbst. Diese Mechanik ist vorhanden und wirkt ab dem Produktivstart; bis dahin führt der Auftragnehmer Löschungen und Anonymisierungen auf Weisung des Auftraggebers durch.

3. Ablauf nach Vertragsende

1. **Tag 0 – Vertragsende.** Die Plattform bleibt für den Auftraggeber im Lesemodus erreichbar; der Auftragnehmer stellt alle Daten zum Abruf bereit: jede Liste als CSV, jedes Dokument mit allen Versionen, das Änderungsprotokoll als JSON.
2. **Bis Tag 30 – Übergabe.** Der Auftraggeber ruft die Daten ab oder bestätigt in Textform, dass er sie nicht benötigt. Auf Wunsch übergibt der Auftragnehmer sie auf einem vereinbarten Weg.
3. **Tag 30 – Löschung.** Der Auftragnehmer löscht alle Daten des Auftraggebers einschließlich Dokumente und Konfiguration (Mandant, Benutzer, Schlüssel, Zugangsdaten zu Carriern) – früher, sobald der Auftraggeber die Übergabe bestätigt hat. Ausnahmen: Daten, für die eine gesetzliche Aufbewahrungspflicht des Auftragnehmers besteht (dann nur eingeschränkte Verarbeitung), und das Archiv des Änderungsprotokolls, das nach Ziffer 1 sieben Jahre ab Archivierung unveränderlich bleibt; es wird dem Auftraggeber übergeben, ist danach für niemanden mehr abrufbar und wird nach Ablauf automatisch gelöscht.
4. **Bis Tag 44 – Sicherungen.** Die Sicherungen der Datenbank laufen durch Rotation aus.
5. **Bestätigung.** Der Auftragnehmer bestätigt den Vollzug der Löschung in Textform mit Datum und Umfang.

OpexGuard GbR · Pommernstr. 12, 67454 Haßloch · info@opexguard.de · www.opexguard.de/sicherheit/avv