

Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO – Anlage 2 zum Auftragsverarbeitungsvertrag

Auftragsverarbeiter	Frank Stolzenburg – claimandgain, Itzweg 7, 38120 Braunschweig, Deutschland, kontakt@claimandgain.de
Gegenstand	Betrieb der Software-as-a-Service-Anwendung claimandgain (Reklamations- und Abweichungsmanagement) auf einem virtuellen Server bei IONOS SE in Deutschland
Fassung vom	09.10.2026, Version 1.5 (ersetzt Version 1.4 vom 09.10.2026)
Nächste Überprüfung	09.10.2027, außerdem bei jeder wesentlichen Änderung der Infrastruktur

Änderungen gegenüber Version 1.4: Entwürfe ungespeicherter Eingaben an das Benutzerkonto gebunden (1.3).

Änderungen in Version 1.4 gegenüber Version 1.3: Zugriffsregel und Pseudonymisierung für das Modul Audit (1.3, 1.5).

Änderungen in Version 1.3 gegenüber Version 1.2: Betreiberdaten und Zugangsgeheimnisse auf dem verschlüsselten Datenträger; Entsperrung des Datenträgers über einen gesonderten Schlüsselservers statt einer Schlüsseldatei auf dem Server, Notfall-Passphrase nur außerhalb des Servers; Jahressicherungen ohne Mandantendaten, Mandantendaten höchstens 13 Monate in Sicherungen; Betreiberdaten in allen Sicherungen.

Änderungen in Version 1.2 gegenüber Version 1.1: Sicherungen ausschließlich in Deutschland; automatische Löschung abgelaufener Demo-Mandanten.

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

1.1 Zutrittskontrolle

- Die Server stehen in ISO-27001-zertifizierten Rechenzentren der IONOS SE in Deutschland; der Schlüsselservers für die Datenträgerverschlüsselung (siehe 2.1) steht in einem Rechenzentrum der Hetzner Online GmbH in Deutschland. Der physische Zutritt unterliegt den Sicherheitsmaßnahmen des jeweiligen Rechenzentrumsbetreibers (Zutrittskontrolle, Videoüberwachung, Sicherheitspersonal).
- Der Betreiber hat keinen physischen Zugang zur Hardware; die Administration erfolgt ausschließlich über verschlüsselte Fernverbindungen.
- Arbeitsplatz des Betreibers: Windows-Rechner mit Benutzeranmeldung und Festplattenverschlüsselung (BitLocker).

1.2 Zugangskontrolle

- Serveradministration (Anwendungsserver und Schlüsselservers) ausschließlich über SSH mit Schlüsselauthentifizierung; die Passwort-Anmeldung per SSH ist deaktiviert. Der private Schlüssel liegt auf dem verschlüsselten Arbeitsplatz des Betreibers und als Sicherungskopie außerhalb des Rechners. Notfallzugang über die Konsole des Hosting-Anbieters.
- Anmeldung im Portal mit E-Mail-Adresse und Passwort; Passwörter werden ausschließlich kryptografisch gehasht gespeichert (kein Klartext, keine Wiederherstellbarkeit).
- Begrenzung von Anmeldeversuchen je Konto (Sperrung für 15 Minuten nach wiederholten Fehlversuchen) und je IP-Adresse; die Zähler werden nur im Arbeitsspeicher gehalten und nirgends angezeigt.

- Automatische Abmeldung nach Inaktivität (Mandant wählt 15 bis 480 Minuten, Voreinstellung 60 Minuten; Betreiberkonto fest 15 Minuten).
- Betreiberzugang (Superadmin) zusätzlich mit Zweitfaktor (TOTP).
- Registrierung nur mit Bestätigung der E-Mail-Adresse; Selbstregistrierung mit Freemail-Adressen ist gesperrt; Firmenregistrierungen von Lieferanten und Kunden werden vom Administrator des Mandanten freigegeben.
- Sitzungen über kurzlebige, signierte Token; Token werden nie in URLs übertragen und erscheinen daher nicht in Protokollen oder Browserverläufen.

1.3 Zugriffskontrolle

- Rollenmodell mit serverseitiger Prüfung jeder Anfrage über einen zentralen Zugriffs-Guard: Administrator, Mitarbeiter, Lesezugang (Mandant); Lieferant und Kunde (Externe) sehen ausschließlich Vorgänge der eigenen Firma.
- Fachliche Sperren werden serverseitig durchgesetzt (eingereichte Disziplinen sind für Externe nicht mehr änderbar, auch nicht über die Schnittstelle).
- Dateianhänge werden nur nach Authentifizierung ausgeliefert.
- Entwürfe sind serverseitig an das Benutzerkonto gebunden; andere Konten einschließlich Administratoren erhalten keinen Zugriff.
- Das Betreiberkonto hat keinen Zugriff auf Benutzerlisten, Verläufe oder Inhalte der Mandanten und kann sich nicht als Mandantenbenutzer anmelden; Zugriffe des Betreibers auf Versandprotokolle der Mandanten werden protokolliert.
- Antworten der Schnittstelle enthalten nur die Felder, die die jeweilige Rolle sehen darf (kein Ausliefern verdeckter Personendaten an Externe).
- Modul Audit: Feststellungen sind für interne Konten lesbar; bearbeiten dürfen nur die Rollen im Vorgang (Prozesseigner oder aktiver Vertreter, Verantwortliche ihrer eigenen Maßnahme, Auditleitung und Co-Auditoren) sowie Administratoren des Auftraggebers; handelt ein Administrator an Stelle des Prozesseigners, hält der Verlauf das fest. Wer Eigner des Prozesses ist, entscheidet nicht über Feststellungen zu diesem Prozess. Lieferanten und Kunden haben keinen Zugang zu Audits.

1.4 Trennungskontrolle

- Jeder Mandant erhält eine eigene Datenbank in einem eigenen Verzeichnis; eine Vermischung von Mandantendaten ist technisch ausgeschlossen. Betreiberdaten liegen in einem gesonderten Bereich.
- Entwicklungs- und Testsysteme sind von der Produktion getrennt; Tests laufen gegen lokale Kopien ohne Echtdaten. Der öffentliche Demo-Mandant enthält ausschließlich Musterdaten.

1.5 Pseudonymisierung (Art. 25 und 32 DSGVO)

- Der Verlauf einer Reklamation speichert den Akteur als dauerhafte Kontokennung und zeigt ihn in der Voreinstellung als Kürzel je Vorgang („Mitarbeiter A“); Klarnamen erscheinen nur nach einem protokollierten Einblenden mit Pflichtbegründung durch einen Administrator des Mandanten.
- Externe (Lieferanten, Kunden) sehen keine Namen von Beschäftigten des Mandanten außer den als Ansprechpartner benannten Erstellern und Beantwortern; E-Mails an Externe enthalten keine internen Adressen.
- Beim Entfernen eines Kontos werden E-Mail-Adresse, Funktion und Passwort gelöscht; im Verlauf verbleibt eine neutrale Kennung.
- Server-Journal ohne Benutzerkennungen und ohne E-Mail-Adressen (Ausnahme: endgültig unzustellbare Mails); Webserver-Zugriffsprotokoll mit anonymisierten IP-Adressen; Mail-Zähler des Betreibers nur mit gehashten Adressen.

- Modul Audit: Der Verlauf einer Feststellung wird wie der einer Reklamation pseudonymisiert. Fristerinnerungen und Eskalationen nennen Rollen und Vorgänge, keine Namen; Eskalationen gehen als eigene Mail ohne den Prozesseigner. Die Übersicht „Meine offenen Punkte“ ist nur für das eigene Konto abrufbar und wird nicht gespeichert. Berichte nach außen nennen Verantwortliche nur mit ihrer Funktion.

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

2.1 Weitergabekontrolle

- Alle Verbindungen zum Portal ausschließlich über TLS (HTTPS) mit Sicherheits-Kopfzeilen; die gesetzten Kopfzeilen sind in Anhang A aufgeführt und werden bei jeder Auslieferung automatisiert gegen den Live-Server geprüft.
- E-Mail-Versand über TLS; Absenderauthentifizierung mit SPF, DKIM und DMARC.
- Mandantendaten, Betreiberdaten (Abrechnungs-, Partner- und Protokolldaten, lokale Sicherungsarchive) und alle Zugangsgeheimnisse der Anwendung liegen auf einem gesonderten, mit LUKS verschlüsselten Datenträger. Auf dem Server liegt kein Schlüssel für diesen Datenträger: Er wird beim Start über einen eigenen Schlüsselservice (Tang) bei einem anderen Anbieter entsperrt, der nur Anfragen dieses Servers annimmt. Wer nur die Datenträger des Servers erlangt, kann die Daten nicht entschlüsseln. Ist der Schlüsselservice nicht erreichbar, erhält der Betreiber nach fünf Minuten einen Alarm und entsperrt den Datenträger mit einer Notfall-Passphrase. Gegen Zugriffe auf den laufenden Server wirken die Maßnahmen der Zugangs- und Zugriffskontrolle (1.2, 1.3).
- Einzige Ausnahme auf dem unverschlüsselten Systemdatenträger: die Zugangsdaten des Postfachs für Systemmeldungen, damit Alarmlisten auch bei gesperrtem Datenträger versendet werden können.
- Sicherungen werden vor der Übertragung clientseitig verschlüsselt (rclone crypt) und verschlüsselt beim Sicherungsdienstleister abgelegt.
- Die Notfall-Passphrase des Datenträgers wird ausschließlich außerhalb des Servers aufbewahrt; Sicherungspasswort, Konfigurationsgeheimnisse und Zweitfaktor-Wiederherstellungscodes zusätzlich dort. Ablage jeweils in einem Passwort-Manager auf dem verschlüsselten Arbeitsplatz des Betreibers und als Offline-Kopie.

2.2 Eingabekontrolle

- Verlauf je Reklamation: jedes fachliche Ereignis mit Zeitpunkt und Akteur-Kennung, unveränderlich (nur Anfügen).
- Auflösungsprotokoll: jedes Einblenden von Namen, jeder Export mit Namen und jede Änderung der Datenschutz-Einstellung mit Datum, Administrator, Vorgang und Begründung.
- Löschartikellprotokoll gelöschter Reklamationen; E-Mail-Versandprotokoll mit Empfänger, Zeitpunkt und Zustellstatus.
- Änderungen an der Software nur über versionierte Auslieferungen mit Prüfkette (siehe 4.3).

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

3.1 Verfügbarkeitskontrolle

- Tägliche verschlüsselte Sicherung aller Mandantendaten und der Betreiberdaten an einen räumlich getrennten Speicher (Hetzner Online GmbH, Rechenzentrum in Deutschland) nach dem Generationenprinzip: tägliche Sicherungen 30 Tage, monatliche Sicherungen 13 Monate. Jährliche Sicherungen enthalten nur Daten mit langer Aufbewahrungspflicht (Abrechnungsdaten, Partnerabrechnung, Sperrliste der Direktansprache) und keine Mandantendaten; sie werden 10 Jahre aufbewahrt und nie automatisch gelöscht. Mandantendaten sind damit höchstens 13 Monate in Sicherungen enthalten.

- Überwachung der Sicherungsläufe: Bleibt eine erfolgreiche Sicherung länger als 36 Stunden aus oder ist der verschlüsselte Datenträger nicht eingehängt, erhält der Betreiber einen Alarm; der wöchentliche Betriebsbericht enthält den Stand der Sicherungen.
- Tägliche Prüfung, ob der Schlüsselservers erreichbar ist und die Schlüssel ankündigt, an die der Datenträger gebunden ist; Alarm bei Abweichung, Stand im wöchentlichen Betriebsbericht. Der Schlüsselservers startet nach Sicherheitsaktualisierungen zu einer anderen Zeit neu als der Anwendungsservers.
- Externe Verfügbarkeitsüberwachung (UptimeRobot) für Landingpage und Portal.
- Automatische Sicherheitsaktualisierungen des Betriebssystems mit geplantem Neustart außerhalb der Geschäftszeiten.
- Schutz vor Versandschleifen: Mail-Anomalie-Alarm bei mehr als 20 Mails an eine Adresse oder mehr als 200 Mails je Mandant und Tag; Fristerinnerungen mit Versandmarker gegen Wiederholung.
- Begrenzung der Anfragen je IP-Adresse und je Konto (Rate-Limiting).

3.2 Wiederherstellbarkeit

- Wiederherstellung einzelner Mandanten aus der Sicherung; vierteljährliche Wiederherstellungsprobe mit Protokoll (skriptgestützt: Rücksicherung eines Mandanten in eine getrennte Umgebung, Vergleich der Datenbestände mit dem Live-System). Erste Probe: September 2026.
- Daten in Sicherungen werden nicht einzeln gelöscht, sondern laufen mit der jeweiligen Sicherung aus. Wird eine Sicherung zurückgespielt, werden die seit ihrer Erstellung gelöschten Daten erneut gelöscht.
- Quellcode als privates Repository mit Zweitfaktor extern gesichert; jede Auslieferung ist mit einem Versionsstempel versehen und lässt sich auf den vorherigen Stand zurücksetzen.

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

4.1 Datenschutz-Management

- Verzeichnis von Verarbeitungstätigkeiten, Auftragsverarbeitungsvertrag und dieses TOM-Dokument werden jährlich und bei wesentlichen Änderungen überprüft; Fassungen sind datiert und versioniert.
- Ein Informationssicherheits-Managementsystem nach ISO/IEC 27001 befindet sich im Aufbau (Geltungsbereich: Betrieb von claimandgain).
- Der Betreiber ist Ein-Personen-Betrieb; es gibt keine weiteren Beschäftigten mit Datenzugang. Werden künftig Personen eingebunden, werden sie auf Vertraulichkeit verpflichtet und in die TOM eingewiesen.

4.2 Vorfallmanagement

- Sicherheits- und Datenschutzvorfälle werden analysiert, behoben, durch einen Nachweistest abgesichert und im Entwicklungsprotokoll dokumentiert.
- Verletzungen des Schutzes personenbezogener Daten werden dem Auftraggeber unverzüglich, spätestens 48 Stunden nach Kenntnis, gemeldet (siehe AVV § 8).

4.3 Datenschutz durch Technikgestaltung und Voreinstellungen (Art. 25 DSGVO)

- Voreinstellung „Pseudonym“ für neue Mandanten; Namensauflösung nur mit Begründung und Protokoll.
- Keine Auswertungen je Person, keine Anmeldeprotokolle; Kennzahlen nur nach Lieferant, Kunde, Fehlerart, Prozess, Status und Zeitraum.

- Automatisierte Aufbewahrungsfristen: E-Mail-Versandprotokoll 12 Monate, Auflösungsprotokoll 24 Monate, Server-Journal 30 Tage, Webserver-Zugriffsprotokoll 7 Tage, Mail-Zähler 90 Tage, Demo-Mandanten ohne Vertragsschluss 3 Monate nach Ablauf (mit Vorankündigung an den Betreiber).
- Jede Auslieferung durchläuft eine automatisierte Prüfkette (Typprüfung, Funktionstests, Sicherheits-Schnellcheck, Datenschutz-Test): Der Datenschutz-Test belegt bei jeder Auslieferung, dass keine Kennzahl je Person existiert, keine Anmeldeprotokolle geführt werden, Externe keine Namen anderer Beschäftigter erhalten, jede Namensauflösung protokolliert wird und die dokumentierten Fristen mit dem Code übereinstimmen. Schlägt ein Test fehl, wird nicht ausgeliefert.

4.4 Auftragskontrolle

- Unterauftragsverarbeiter werden nur mit Auftragsverarbeitungsvertrag eingesetzt und sind in Anlage 1 des AVV aufgeführt: IONOS SE (Hosting), Hetzner Online GmbH (Sicherungen), DeepL SE (Übersetzung von Freitexten auf Anforderung des Nutzers, auf Grundlage der DeepL-Datenverarbeitungsvereinbarung). Der Schlüsselserver (Hetzner Online GmbH) verarbeitet keine personenbezogenen Daten und ist kein Unterauftragsverarbeiter.
- Weisungen des Auftraggebers werden über die Funktionen des Portals (Einstellungen, Kontoverwaltung, Löschung) und in Textform entgegengenommen.
- Nach Vertragsende werden die Mandantendaten innerhalb von 30 Tagen gelöscht; Sicherungen laufen nach höchstens 13 Monaten aus.

Anhang A - Sicherheits-Kopfzeilen des Portals

Kopfzeile	Wert
Strict-Transport-Security	max-age=31536000; includeSubDomains
Content-Security-Policy	default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; font-src 'self' data;; connect-src 'self'; frame-src 'self' blob;; object-src 'none'; base-uri 'self'; form-action 'self'; frame-ancestors 'self'
X-Frame-Options	SAMEORIGIN
X-Content-Type-Options	nosniff
Referrer-Policy	strict-origin-when-cross-origin
Permissions-Policy	camera=(), microphone=(), geolocation=()

Diese Tabelle wird beim Erzeugen des Dokuments aus der Serverkonfiguration eingesetzt und bei jeder Auslieferung gegen den Live-Server geprüft.