

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

Version 1.3 vom 16.10.2026 · Muster des Betreibers, vor Verwendung anwaltlich zu prüfen.
Geschweifte Klammern werden vom Portal mit den Daten des Mandanten gefüllt.

Änderungen gegenüber Version 1.2: Anlage 3 um das Organigramm ergänzt (Organisationseinheit am Konto, Leitung von Organisationseinheiten).

Änderungen in Version 1.2 gegenüber Version 1.1: Anlage 3 und § 9 Abs. 2 um das Modul Audit ergänzt.

zwischen

{MANDANT_FIRMA}, {MANDANT_ANSCHRIFT} – nachfolgend Auftraggeber (Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO) –

und

Frank Stolzenburg – claimandgain, Itzweg 7, 38120 Braunschweig, Deutschland – nachfolgend Auftragnehmer (Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO) –

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer betreibt für den Auftraggeber die Software-as-a-Service-Anwendung claimandgain zum Reklamations- und Abweichungsmanagement (nachfolgend „Portal“) unter der Mandantenadresse {MANDANT_SUBDOMAIN}.claimandgain.de. Dieser Vertrag regelt die Verarbeitung personenbezogener Daten, die der Auftragnehmer dabei im Auftrag des Auftraggebers vornimmt.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Nutzungsvertrags über das Portal (Abonnement). Er endet mit dem Nutzungsvertrag, ohne dass es einer gesonderten Kündigung bedarf.

(3) Gegenstand, Art und Zweck der Verarbeitung, die Kategorien betroffener Personen und die Kategorien personenbezogener Daten sind in Anlage 3 beschrieben.

§ 2 Weisungsgebundenheit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet ist; in diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

(2) Weisungen erteilt der Auftraggeber über die Funktionen des Portals (insbesondere Einstellungen, Konto- und Berechtigungsverwaltung, Löschung von Vorgängen und Konten) sowie in Textform an kontakt@claimandgain.de. Weisungsberechtigt sind die Administratoren des Auftraggebers im Portal.

(3) Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen.

(4) Eine Verarbeitung in einem Drittland findet nicht statt. Die Verarbeitung erfolgt ausschließlich in Mitgliedstaaten der Europäischen Union (siehe Anlage 1).

§ 3 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er stellt sicher, dass die Nutzung des Portals im Verhältnis zu seinen Beschäftigten, Lieferanten und Kunden rechtmäßig ist, insbesondere hinsichtlich bestehender Mitbestimmungsrechte. Der Auftragnehmer stellt hierzu ein Informationsblatt für den Betriebsrat und eine Muster-Betriebsvereinbarung bereit.
- (2) Der Auftraggeber wählt die Datenschutz-Einstellungen des Portals (insbesondere den Modus der Namensanzeige im Verlauf) eigenverantwortlich; die Voreinstellung ist „Pseudonym“.
- (3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 4 Vertraulichkeit

- (1) Der Auftragnehmer verpflichtet sich zur Vertraulichkeit. Personen, die er künftig mit der Verarbeitung betraut, verpflichtet er vor Aufnahme der Tätigkeit auf Vertraulichkeit und macht sie mit den für sie maßgeblichen Datenschutzvorschriften vertraut.
- (2) Zum Zeitpunkt des Vertragsschlusses hat ausschließlich der Auftragnehmer selbst Zugang zu den Systemen; weitere Beschäftigte gibt es nicht.

§ 5 Sicherheit der Verarbeitung

- (1) Der Auftragnehmer trifft die in Anlage 2 (Technische und organisatorische Maßnahmen) beschriebenen Maßnahmen nach Art. 32 DSGVO und hält sie für die Vertragsdauer aufrecht.
- (2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert und dem Auftraggeber in einer neuen Fassung der Anlage 2 zur Verfügung gestellt.

§ 6 Unterauftragsverarbeiter

- (1) Der Auftraggeber genehmigt die in Anlage 1 aufgeführten Unterauftragsverarbeiter.
- (2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform mindestens vier Wochen im Voraus. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichen Grund widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Bei Widerspruch kann jede Partei den Nutzungsvertrag außerordentlich zum Wirksamwerden der Änderung kündigen.
- (3) Der Auftragnehmer schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind. Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Erfüllung der Pflichten seiner Unterauftragsverarbeiter.
- (4) Keine Unterauftragsverarbeitung im Sinne dieses Vertrags sind Leistungen Dritter, die der Auftragnehmer als eigener Verantwortlicher in Anspruch nimmt (z. B. Zahlungsabwicklung des Abonnements über Stripe Payments Europe Ltd., Telekommunikation, Verfügbarkeitsüberwachung ohne Zugriff auf Inhaltsdaten).

§ 7 Rechte der betroffenen Personen

- (1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflichten nach Art. 12 bis 22 DSGVO. Das Portal stellt hierfür insbesondere bereit: Einsicht, Änderung und Löschung von Vorgängen durch den Auftraggeber, das Entfernen von Konten mit Anonymisierung im Verlauf, den Export von Vorgängen als PDF sowie das Auflösungsprotokoll.
- (2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst, sofern der Auftraggeber nichts anderes bestimmt.

§ 8 Unterstützungspflichten und Meldung von Verletzungen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

(2) Verletzungen des Schutzes personenbezogener Daten, die Daten des Auftraggebers betreffen, meldet der Auftragnehmer dem Auftraggeber unverzüglich, spätestens 48 Stunden nach Kenntnis, an die im Portal hinterlegte Adresse des Administrators. Die Meldung enthält, soweit bekannt, Art und Umfang der Verletzung, betroffene Datenkategorien und Personen, wahrscheinliche Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen. Nachträglich bekannt werdende Informationen werden unverzüglich nachgereicht.

§ 9 Löschung und Rückgabe

(1) Nach Beendigung des Nutzungsvertrags löscht der Auftragnehmer sämtliche im Auftrag verarbeiteten personenbezogenen Daten des Auftraggebers innerhalb von 30 Tagen, sofern nicht eine gesetzliche Aufbewahrungspflicht entgegensteht. Sicherungskopien laufen entsprechend ihrer Vorhaltung aus und werden nicht gesondert wiederhergestellt.

(2) Der Auftraggeber kann bis zur Beendigung seine Vorgänge über die Exportfunktionen des Portals sichern (8D-Report je Reklamation, Berichte je Audit). Eine darüber hinausgehende Herausgabe der Datenbank in maschinenlesbarer Form kann der Auftraggeber bis zum Vertragsende in Textform verlangen.

(3) Auf Verlangen bestätigt der Auftragnehmer die Löschung in Textform.

§ 10 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO erforderlich sind. Hierzu gehören insbesondere dieses Dokument mit seinen Anlagen, das Verzeichnis der Verarbeitungstätigkeiten (Teil B) auf Anfrage sowie der Bericht des automatisierten Datenschutz-Tests, der bei jeder Auslieferung des Portals läuft.

(2) Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrags zu überprüfen. Kontrollen erfolgen vorrangig durch Einholung schriftlicher Auskünfte und Nachweise; Prüfungen vor Ort sind nach vorheriger Anmeldung mit angemessener Frist (in der Regel vier Wochen) während der üblichen Geschäftszeiten möglich, ohne den Betrieb für andere Mandanten zu beeinträchtigen. Der Auftragnehmer kann Zertifizierungen oder Prüfberichte unabhängiger Stellen als gleichwertigen Nachweis vorlegen.

§ 11 Haftung

Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Nutzungsvertrags.

§ 12 Schlussbestimmungen

(1) Dieser Vertrag wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO), indem ein Administrator des Auftraggebers ihn im Portal annimmt. Das Portal protokolliert Version, Datum und annehmendes Konto: {ANNAHME_DATUM}, {ANNAHME_KONTO}.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag gehen die Regelungen dieses Vertrags vor, soweit sie den Datenschutz betreffen.

(3) Änderungen dieses Vertrags bedürfen der Textform. Der Auftragnehmer kann eine neue Fassung im Portal zur Annahme vorlegen; bis zur Annahme gilt die bisherige Fassung fort.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage 1 - Unterauftragsverarbeiter

Unternehmen	Anschrift	Leistung	Ort der Verarbeitung
IONOS SE	Elgendorfer Straße 57, 56410 Montabaur, Deutschland	Hosting des virtuellen Servers, E-Mail-Postfächer für den Systemversand	Deutschland
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Deutschland	Speicherung verschlüsselter Sicherungen (die Sicherungen sind vor der Übertragung verschlüsselt; der Unterauftragsverarbeiter hat keinen Zugriff auf Inhalte)	Europäische Union (Deutschland oder Finnland)
DeepL SE	Maarweg 165, 50825 Köln, Deutschland	Maschinelle Übersetzung von Freitexten, ausschließlich auf Anforderung des jeweiligen Nutzers, auf Grundlage der DeepL-Datenverarbeitungs- vereinbarung; die Texte werden nach der Übersetzung nicht gespeichert	Europäische Union

Keine Unterauftragsverarbeiter im Sinne von § 6 Abs. 4: Stripe Payments Europe Ltd.
(Zahlungsabwicklung des Abonnements, eigener Verantwortlicher), UptimeRobot
(Verfügbarkeitsüberwachung ohne Zugriff auf Inhaltsdaten).

Anlage 2 - Technische und organisatorische Maßnahmen

Siehe das gesonderte Dokument „Technische und organisatorische Maßnahmen (TOM)“ in der jeweils gültigen Fassung, abrufbar für Administratoren unter Einstellungen → Datenschutz.

Anlage 3 – Gegenstand der Verarbeitung

Gegenstand	Betrieb des Portals claimandgain für den Auftraggeber einschließlich der Zugänge seiner Lieferanten und Kunden
Art und Zweck	Speicherung, Anzeige, Änderung und Löschung von Konto- und Vorgangsdaten; Benutzer- und Berechtigungsverwaltung; Versand systembezogener E-Mail-Benachrichtigungen, Fristerinnerungen und Eskalationen; Erzeugung von Berichten (PDF); Protokollierung fachlicher Ereignisse je Reklamation und je Audit-Feststellung mit pseudonymisierter Akteursangabe; protokollierte Namensauflösung; Übersetzung von Freitexten auf Anforderung; automatische Löschläufe; Datensicherung; Wartung und Störungsbeseitigung. Zweck: Reklamations- und Abweichungsmanagement des Auftraggebers einschließlich der Bearbeitung von Feststellungen aus Audits (Modul Audit, soweit genutzt)
Kategorien betroffener Personen	Beschäftigte des Auftraggebers; Beschäftigte von Lieferanten und Kunden des Auftraggebers; sonstige in Vorgangsdaten benannte Personen (z. B. Teammitglieder im 8D-Report oder in einer Audit-Feststellung)
Kategorien personenbezogener Daten	Kontodaten (dienstliche E-Mail-Adresse, Funktion, Rolle, Sprache, Firmenzuordnung, Auditor-Kennzeichen, Organisationseinheit); Zuständigkeiten (Ersteller, Beantworter; beim Modul Audit Auditleitung und Co-Auditoren, Prozesseigner und Vertreter mit Enddatum der Vertretung, Verantwortliche von Maßnahmen; Leitung von Organisationseinheiten); Verlauf je Reklamation und je Feststellung (Ereignis, Zeitpunkt, Akteur als Kennung); E-Mail-Versandprotokoll; Auflösungsprotokoll; Löschartikel; Inhaltsdaten der Reklamations- und Auditbearbeitung einschließlich Dateianhängen und Fotos, Maßnahmen, Nachweisen, Wirksamkeitsprüfungen, Rückfragen und internen Notizen
Besondere Kategorien (Art. 9 DSGVO)	Nicht vorgesehen. Der Auftraggeber stellt sicher, dass in Freitexten und Anhängen keine besonderen Kategorien personenbezogener Daten erfasst werden
Aufbewahrung	Vorgangsdaten (Reklamationen, Audits, Feststellungen): bis zur Löschung durch den Auftraggeber (Audits nur, solange sie im Entwurf sind) bzw. bis Vertragsende; E-Mail-Versandprotokoll 12 Monate; Auflösungsprotokoll 24 Monate; Server-Journal 30 Tage; Webserver-Zugriffsprotokoll 7 Tage; Enddatum einer Vertretung: bis zum Ablauf; entfernte Konten: sofortige Löschung von E-Mail-Adresse, Funktion und Passwort