

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

zwischen

– nachfolgend „Auftraggeber“ genannt –

und der

Setago.io GmbH
Brunnengasse 16
90402 Nürnberg

– nachfolgend „Auftragnehmer“ genannt –

gemeinsam auch „Parteien“ genannt.

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Nutzung der cloudbasierten Softwarelösung Setago durch den Auftraggeber.

Setago ist eine SaaS-Lösung zur Digitalisierung von Arbeitsanweisungen, Werkerassistenzprozessen, Prüf- und Traceability-Abläufen sowie optional zur Anbindung sensorischer Hardware wie Pick-by-Light, Pick-by-Weight, Scanner, Schrauber, Edge-Gateways oder vergleichbarer Geräte.

Der Auftraggeber ist datenschutzrechtlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers und ist insoweit Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO.

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand dieses Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Zusammenhang mit der Bereitstellung, dem Betrieb, der Wartung, dem Support und der Weiterentwicklung der SaaS-Lösung Setago.

Die nähere Beschreibung des Auftrags, der Art und Zwecke der Verarbeitung, der Kategorien personenbezogener Daten sowie der Kategorien betroffener Personen ergibt sich aus **Anlage 1 – Gegenstand der Verarbeitung**.

1.2 Dauer

Die Dauer dieses Auftrags richtet sich nach der Laufzeit des zwischen den Parteien bestehenden Hauptvertrags über die Nutzung der Setago-Software.

Endet der Hauptvertrag, endet grundsätzlich auch diese Vereinbarung, soweit keine gesetzlichen Aufbewahrungspflichten oder fortwirkenden Pflichten aus dieser Vereinbarung bestehen.

1.3 Vorrang

Bei Widersprüchen zwischen dieser Vereinbarung und sonstigen vertraglichen Regelungen gehen die Regelungen dieser Vereinbarung in datenschutzrechtlichen Fragen vor.

2. Konkretisierung des Auftrags

2.1 Art und Zweck der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen, insbesondere zur:

- Bereitstellung der Setago-Webanwendung,
- Verwaltung von Benutzerkonten, Rollen und Berechtigungen,
- Authentifizierung und Autorisierung von Nutzern,
- Speicherung und Anzeige von Arbeitsanweisungen, Artikeln, Bildern, Dateien, Sequenzen und Prozessdaten,
- Erfassung und Speicherung von Traceability-Daten, soweit vom Auftraggeber genutzt,
- Bereitstellung von Support-, Wartungs- und Betriebsleistungen,
- Sicherstellung von Verfügbarkeit, Monitoring, Fehleranalyse und IT-Sicherheit,
- Bereitstellung optionaler Schnittstellen und Hardware-Anbindungen, insbesondere über Edge-Gateways.

2.2 Ort der Verarbeitung

Die produktive Verarbeitung von Kundendaten erfolgt grundsätzlich innerhalb der Europäischen Union, insbesondere in der AWS-Region eu-central-1 / Frankfurt am Main.

Soweit technisch erforderlich, können Failover-, Backup-, Wiederherstellungs- oder Redundanzmechanismen in weiteren europäischen AWS-Regionen genutzt werden, insbesondere in Regionen innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums. Hierzu können insbesondere europäische Regionen wie eu-west-1 / Irland oder eu-north-1 / Stockholm gehören, soweit diese im jeweiligen Betriebs- oder Backup-Konzept aktiviert oder konfiguriert sind.

Eine Verarbeitung in Drittstaaten findet nur statt, soweit die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Weisungsrecht des Auftraggebers

3.1 Verarbeitung nur auf Weisung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit keine gesetzliche Verpflichtung zur Verarbeitung besteht.

Die Weisung ergibt sich grundsätzlich aus:

- dem Hauptvertrag,
- dieser Vereinbarung,
- den vom Auftraggeber vorgenommenen Einstellungen innerhalb der Anwendung,
- schriftlichen oder in Textform erteilten Einzelweisungen.

3.2 Form der Weisung

Weisungen können schriftlich oder in Textform, insbesondere per E-Mail, erteilt werden.

Mündliche Weisungen sind vom Auftraggeber unverzüglich mindestens in Textform zu bestätigen.

3.3 Unzulässige Weisungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.

Der Auftragnehmer ist berechtigt, die Durchführung einer solchen Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wurde.

4. Pflichten des Auftragnehmers

4.1 Verarbeitung im Auftrag

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung, des Hauptvertrags und der dokumentierten Weisungen des Auftraggebers.

4.2 Vertraulichkeit

Der Auftragnehmer stellt sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Zugriff auf personenbezogene Daten erfolgt nur durch berechtigte Personen und nur soweit dies zur Vertragserfüllung, zum Betrieb, zur Wartung, zur Fehleranalyse, zur IT-Sicherheit oder zum Support erforderlich ist.

4.3 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 28 Abs. 3 lit. c und Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die zum Zeitpunkt des Vertragsschlusses geltenden technischen und organisatorischen Maßnahmen sind in dem separaten Dokument „**Technische und organisatorische Maßnahmen der Setago.io GmbH**“ beschrieben. Dieses Dokument ist Bestandteil dieser Vereinbarung.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer ist berechtigt, einzelne Maßnahmen anzupassen, zu ersetzen oder weiterzuentwickeln, sofern dadurch das bestehende Sicherheitsniveau nicht unterschritten wird.

Wesentliche Änderungen der technischen und organisatorischen Maßnahmen werden dokumentiert. Auf Anfrage stellt der Auftragnehmer dem Auftraggeber die jeweils aktuelle Fassung der technischen und organisatorischen Maßnahmen zur Verfügung.

4.4 Zugriffsbeschränkung

Der Auftragnehmer stellt sicher, dass Zugriff auf produktive Systeme nur über rollenbasierte Accounts und nur durch autorisierte Personen erfolgt.

Interne Zugriffsrechte werden nach dem Need-to-know-Prinzip vergeben.

4.5 Support-Zugriff

Ein Support-Zugriff durch den Auftragnehmer erfolgt nur, soweit dies zur Fehleranalyse, Wartung, Unterstützung des Auftraggebers oder Sicherstellung des Betriebs erforderlich ist.

Support-Zugänge werden geschützt verwaltet und nicht für den regulären Betrieb durch Endnutzer verwendet.

4.6 Verzeichnis von Verarbeitungstätigkeiten

Der Auftragnehmer führt, soweit gesetzlich erforderlich, ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

4.7 Zusammenarbeit mit Aufsichtsbehörden

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren bei Anfragen oder Prüfungen von Datenschutzaufsichtsbehörden, soweit diese die vereinbarte Auftragsverarbeitung betreffen.

5. Pflichten des Auftraggebers

5.1 Verantwortlichkeit

Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich, insbesondere für:

- die Rechtmäßigkeit der Datenerhebung,
- die Zulässigkeit der Verarbeitung,
- die Information betroffener Personen,
- die Wahrung von Betroffenenrechten,
- die Auswahl der in Setago verarbeiteten Inhalte,
- die Vergabe und Entziehung von Benutzerrechten innerhalb seiner Organisation.

5.2 Benutzerverwaltung

Der Auftraggeber ist verantwortlich für die ordnungsgemäße Verwaltung seiner Benutzer, Rollen und Berechtigungen innerhalb der Anwendung, soweit diese nicht ausdrücklich vom Auftragnehmer übernommen wurde.

Dies umfasst insbesondere:

- Einladung neuer Benutzer,
- Entzug von Benutzerrechten,
- Prüfung aktiver Benutzer,
- Vergabe geeigneter Rollen,
- Entfernung ausgeschiedener oder nicht mehr berechtigter Nutzer.

5.3 Inhalte des Auftraggebers

Der Auftraggeber entscheidet eigenverantwortlich, welche Inhalte, Dateien, Bilder, Artikel, Arbeitsanweisungen, Sequenzen, Prüfprotokolle oder sonstigen Informationen in Setago verarbeitet werden.

Der Auftragnehmer hat keinen Einfluss darauf, ob der Auftraggeber über die vorgesehenen Datenkategorien hinaus weitere personenbezogene Daten in Freitextfeldern, Bildern, Dateien, Dateinamen, Kommentaren oder sonstigen Inhalten verarbeitet.

6. Unterauftragnehmer

6.1 Allgemeine Genehmigung

Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zur Einschaltung von Unterauftragnehmern, soweit diese für die Bereitstellung, den Betrieb, die Wartung, das Hosting, die Überwachung, die Authentifizierung, den Support oder die Sicherheit der Setago-Lösung erforderlich sind.

Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer sind in **Anlage 2 – Unterauftragnehmer** aufgeführt.

6.2 Wechsel oder Hinzunahme von Unterauftragnehmern

Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragnehmern mit angemessener Frist vorab.

Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund gegen die Änderung Einspruch erheben.

Im Fall technischer Störungen, Sicherheitsvorfälle oder zwingender betrieblicher Erfordernisse ist der Auftragnehmer berechtigt, kurzfristig einen Unterauftragnehmer zu ersetzen oder zusätzlich einzusetzen, soweit dies zur Sicherstellung des Dienstbetriebs oder zur Abwehr von Risiken erforderlich ist. Der Auftraggeber wird hierüber unverzüglich informiert.

6.3 Verpflichtung der Unterauftragnehmer

Der Auftragnehmer stellt sicher, dass mit Unterauftragnehmern Vereinbarungen geschlossen werden, die den Anforderungen des Art. 28 DSGVO entsprechen.

Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der datenschutzrechtlichen Pflichten durch Unterauftragnehmer verantwortlich.

7. Unterstützung bei Betroffenenrechten

7.1 Allgemeine Unterstützung

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren bei der Erfüllung von Betroffenenrechten gemäß Art. 12 bis 23 DSGVO, insbesondere bei:

- Auskunft,
- Berichtigung,
- Löschung,
- Einschränkung der Verarbeitung,
- Datenübertragbarkeit.

7.2 Direkte Anfragen betroffener Personen

Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, wird der Auftragnehmer diese Anfrage grundsätzlich an den Auftraggeber verweisen, sofern eine Zuordnung zum Auftraggeber möglich ist.

Der Auftragnehmer wird Anfragen betroffener Personen nicht eigenständig beantworten, soweit er hierzu nicht gesetzlich verpflichtet ist oder vom Auftraggeber entsprechend angewiesen wurde.

8. Unterstützung bei Datenschutz-Folgenabschätzung und vorheriger Konsultation

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren bei der Einhaltung der Pflichten gemäß Art. 35 und Art. 36 DSGVO, soweit die Unterstützung die durch den Auftragnehmer erbrachte Auftragsverarbeitung betrifft.

Dies gilt insbesondere für die Bereitstellung erforderlicher Informationen zu den technischen und organisatorischen Maßnahmen, den Verarbeitungstätigkeiten und den eingesetzten Unterauftragnehmern.

9. Meldung von Datenschutzverletzungen

9.1 Informationspflicht

Der Auftragnehmer informiert den Auftraggeber unverzüglich, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Daten des Auftraggebers betrifft.

9.2 Inhalt der Meldung

Die Meldung enthält, soweit zum Zeitpunkt der Meldung bekannt, insbesondere:

- Art der Verletzung,
- betroffene Datenkategorien,
- betroffene Systeme,
- wahrscheinliche Folgen,
- bereits ergriffene oder vorgeschlagene Maßnahmen,
- Ansprechpartner für Rückfragen.

9.3 Unterstützung

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren bei der Erfüllung etwaiger Melde- und Benachrichtigungspflichten gemäß Art. 33 und Art. 34 DSGVO.

10. Kontrollrechte des Auftraggebers

10.1 Nachweise

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage geeignete Informationen zur Verfügung, um die Einhaltung der Pflichten aus dieser Vereinbarung nachzuweisen.

Dies kann insbesondere erfolgen durch:

- Beschreibung der technischen und organisatorischen Maßnahmen,
- Sicherheits- und Betriebskonzepte,
- Datenschutzdokumentation,
- Audit-Informationen,
- Zertifikate oder geeignete Nachweise, soweit vorhanden.

10.2 Audits

Der Auftraggeber ist berechtigt, nach vorheriger angemessener Ankündigung und während üblicher Geschäftszeiten Prüfungen durchzuführen oder durch geeignete Prüfer durchführen zu lassen.

Audits sind mindestens vier Wochen vorher anzukündigen, soweit kein konkreter Datenschutzvorfall oder eine behördliche Anordnung eine kurzfristigere Prüfung erforderlich macht.

10.3 Vertraulichkeit und Verhältnismäßigkeit

Audits dürfen den Geschäftsbetrieb des Auftragnehmers nicht unangemessen beeinträchtigen.

Der Auftraggeber stellt sicher, dass eingesetzte Prüfer zur Vertraulichkeit verpflichtet sind und keine Wettbewerber des Auftragnehmers sind.

Soweit durch ein Audit erheblicher zusätzlicher Aufwand entsteht, der nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen ist, können die Parteien vor Durchführung des Audits eine angemessene Kostentragung vereinbaren.

11. Löschung und Rückgabe von Daten

11.1 Datenexport

Der Auftraggeber kann während der Vertragslaufzeit Daten aus der Anwendung exportieren, soweit entsprechende Funktionen bereitgestellt werden oder der Export technisch möglich ist.

11.2 Löschung während der Vertragslaufzeit

Der Auftraggeber kann bestimmte Daten innerhalb der Anwendung selbst löschen, insbesondere Artikel, Sequenzen, Arbeitsanweisungen, Dateien oder vergleichbare Inhalte, soweit die Anwendung diese Funktionen bereitstellt.

11.3 Löschung nach Vertragsende

Nach Beendigung des Hauptvertrags werden die Daten des Auftraggebers grundsätzlich für bis zu 60 Tage vorgehalten, um dem Auftraggeber einen Export oder eine Reaktivierung zu ermöglichen.

Nach Ablauf dieser Frist werden die Daten gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Eine frühere Löschung kann der Auftraggeber in Textform verlangen.

11.4 Backups

Sicherheitskopien und Backups werden im Rahmen der bestehenden Backup-Zyklen gelöscht oder überschrieben.

Eine sofortige Löschung aus sämtlichen Backups ist technisch nicht immer möglich. Der Auftragnehmer stellt jedoch sicher, dass Daten aus Backups nicht produktiv wiederhergestellt werden, sofern eine Löschung verlangt wurde, es sei denn, dies ist zur Wiederherstellung der Systemintegrität erforderlich.

11.5 Nachweisdokumentation

Dokumentationen, die dem Nachweis einer ordnungsgemäßen Verarbeitung dienen, können entsprechend gesetzlicher Aufbewahrungspflichten oder berechtigter Nachweiserfordernisse über das Vertragsende hinaus aufbewahrt werden.

12. Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften sowie den Regelungen des Hauptvertrags.

13. Schlussbestimmungen

13.1 Änderungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der Textform.

13.2 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

13.3 Rechtswahl

Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1: Gegenstand der Verarbeitung

1. Beschreibung des Auftrags

Der Auftragnehmer stellt dem Auftraggeber die cloudbasierte Softwarelösung Setago zur Verfügung.

Setago dient insbesondere zur:

- Erstellung und Verwaltung digitaler Arbeitsanweisungen,
- Durchführung von Werkerassistenzprozessen,
- Verwaltung von Artikeln, Bildern, Dateien und Sequenzen,
- Erfassung von Prozess- und Traceability-Daten,
- Verwaltung von Benutzern, Rollen und Berechtigungen,
- optionalen Anbindung von Sensorik und Hardware, zum Beispiel Pick-by-Light, Pick-by-Weight, Scanner, Schrauber, Edge-Gateways oder vergleichbarer Geräte,
- Bereitstellung von Support-, Wartungs-, Monitoring- und Betriebsleistungen.

2. Art der Verarbeitung

Die Verarbeitung umfasst insbesondere:

- Erheben,
- Erfassen,
- Speichern,
- Ordnen,
- Strukturieren,
- Anzeigen,
- Übermitteln innerhalb der Anwendung,
- Bereitstellen,
- Auswerten,
- Protokollieren,
- Löschen,
- Wiederherstellen aus Backups im Störfall.

3. Zweck der Verarbeitung

Zweck der Verarbeitung ist die Bereitstellung und Nutzung der Setago-Software durch den Auftraggeber zur Digitalisierung und Unterstützung von Produktions-, Montage-, Prüf-, Schulungs- oder Qualitätsprozessen.

4. Kategorien personenbezogener Daten

Je nach Nutzung durch den Auftraggeber können folgende personenbezogene Daten verarbeitet werden:

4.1 Benutzer- und Accountdaten

- Name des Benutzers, soweit vom Auftraggeber gepflegt,
- geschäftliche E-Mail-Adresse,
- Benutzerrolle,
- Berechtigungen,
- Tenant-/Organisationszuordnung,
- Login- und Authentifizierungsdaten,
- technische Benutzerkennungen.

4.2 Nutzungs- und Protokolldaten

- Benutzeraktionen innerhalb der Anwendung,
- Änderungen an Rollen und Rechten,
- Ausführung von Arbeitsanweisungen oder Sequenzen,
- Zeitstempel,
- technische Fehler- und Ereignisprotokolle,
- Support- und Monitoringdaten.

4.3 Prozess- und Traceability-Daten

- ausgeführte Arbeitsanweisungen,
- Sequenzdaten,
- verwendete Artikel,
- Mengen,
- Gewichte,
- Zeitstempel,
- Prozessstatus,
- Prüfergebnisse,
- Rückverfolgbarkeitsdaten.

4.4 Inhaltsdaten des Auftraggebers

Soweit vom Auftraggeber eingegeben oder hochgeladen:

- Artikelbezeichnungen,
- Artikelnummern,
- Bilder,
- Dateien,
- Arbeitsanweisungen,
- Kommentare,
- Freitextfelder,
- sonstige vom Auftraggeber bereitgestellte Inhalte.

Der Auftragnehmer hat keinen Einfluss darauf, ob der Auftraggeber in Freitextfeldern, Bildern, Dateinamen, Kommentaren oder hochgeladenen Dokumenten zusätzliche personenbezogene Daten verarbeitet.

5. Kategorien betroffener Personen

Betroffene Personen können insbesondere sein:

- Mitarbeiter des Auftraggebers,
- Produktionsmitarbeiter,
- Administratoren,
- Manager,
- Operatoren,
- externe Dienstleister oder Partner des Auftraggebers mit Benutzerzugang,
- Support-Ansprechpartner des Auftraggebers.

6. Besondere Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO ist durch die Setago-Anwendung nicht vorgesehen.

Der Auftraggeber verpflichtet sich, solche Daten nicht ohne gesonderte Rechtsgrundlage und ohne vorherige Abstimmung in Setago zu verarbeiten.

Anlage 2: Unterauftragnehmer

Die folgende Liste beschreibt die Unterauftragnehmer, die zur Bereitstellung, zum Betrieb, zur Wartung, zur Authentifizierung, zum Monitoring oder zur Absicherung der Setago-Lösung eingesetzt werden können.

Unterauftragnehmer	Sitz / Land	Leistung
Amazon Web Services EMEA SARL / Amazon Web Services, Inc.	EU / USA; produktiver Serverstandort primär eu-central-1 Frankfurt	Cloud-Infrastruktur, Hosting, Datenbankbetrieb, Storage, Netzwerkdienste, Verfügbarkeits- und Sicherheitsdienste
Datadog	EU-Site	Monitoring, technische Protokollierung, Performance- und Fehlerüberwachung
GitLab		Quellcodeverwaltung, CI/CD, Entwicklungs- und Deployment-Prozesse. Keine Verarbeitung personenbezogener Daten.
chargebee	Frankfurt	Nur falls vom Kunden in Anspruch genommen: Abonnementverwaltung, Self-Subscription, Rechnungs- und Zahlungsabwicklung, Lizenz- und Vertragsverwaltung

Anlage 3: Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen des Auftragnehmers sind in dem separaten Dokument

„Technische und organisatorische Maßnahmen der Setago.io GmbH“

in der jeweils gültigen Fassung beschrieben.

Stand bei Vertragsschluss: **11.10.2025**

Dieses Dokument ist Bestandteil dieses Auftragsverarbeitungsvertrags.

Der Auftragnehmer ist berechtigt, die technischen und organisatorischen Maßnahmen fortlaufend an technische, organisatorische oder sicherheitsrelevante Entwicklungen anzupassen, sofern das bestehende Sicherheitsniveau nicht unterschritten wird.