



Data Processing Agreement

Agreement on the processing of personal data on behalf of a controller pursuant to Article 28 GDPR

As of 9 October 2026

between

Controller (controller within the meaning of Art. 4 No. 7 GDPR)	The Processor's customer that has registered on the "Collectu" platform and concluded the Main Agreement. Company name, address and contact details are those provided during registration or stored in the customer account.
--	---

– hereinafter the "Controller" –

and

Processor (processor within the meaning of Art. 4 No. 8 GDPR)	Collectu GmbH Seidenstraße 36 70174 Stuttgart, Germany Commercial register: Local Court of Stuttgart, HRB 803639 Represented by: Dr. Colin Reiff, Dr. Frederik Wulle E-mail (data protection): info@collectu.de
--	--

– hereinafter the "Processor" –

– together the "Parties" –

Recitals

The Controller has registered on the Processor's platform and has concluded with the Processor a contract for the provision and use of the software "Collectu" on the basis of the General Terms and Conditions of Collectu GmbH (hereinafter the "Main Agreement"). In providing these services, the Processor processes personal data on behalf of and on the instructions of the Controller. This agreement specifies the data protection rights and obligations of the Parties and satisfies the requirements of Art. 28(3) GDPR.

The Controller remains solely responsible for the lawfulness of the processing and for safeguarding the rights of data subjects.

Collectu GmbH
Seidenstraße 36
70174 Stuttgart
Germany

Payment Details
Baden-Württembergische Bank
IBAN: DE33600501010405966093
BIC: SOLAEST600

VAT ID: DE461208298
Commercial Register No.: HRB 803639
Register Court: Amtsgericht Stuttgart
CEO: Dr. Colin Reiff und Dr. Frederik Wulle

§ 1 Subject matter, scope and duration of the processing; conclusion of this agreement

- (1) The subject matter of the processing is the provision of the services agreed in the Main Agreement, to the extent that personal data of the Controller are processed in the course thereof.
- (2) The software is provided in a hybrid deployment model: a software component (hereinafter the "Core") is installed and operated within the Controller's infrastructure, while administration, configuration, storage and analysis take place via a cloud platform operated by the Processor (hereinafter the "Hub"). Processing on behalf of the Controller within the meaning of this agreement occurs to the extent that personal data are transmitted to or processed on the Hub, and to the extent that the Processor accesses the Controller's systems or data in the course of support and remote maintenance services.
- (3) The nature and purpose of the processing, the types of personal data and the categories of data subjects are set out exhaustively in Annex 1.
- (4) The term of this agreement corresponds to the term of the Main Agreement. Termination of the Main Agreement also terminates this agreement; obligations which by their nature survive termination (in particular §§ 5, 11 and 13) remain unaffected.
- (5) This agreement is concluded electronically. It becomes effective as soon as the Controller accepts it during registration or when concluding the Main Agreement, or at a later point in time, in particular by ticking a corresponding checkbox. No signature by the Parties is required; conclusion in electronic form satisfies the requirements of Art. 28(9) GDPR.
- (6) The natural person accepting this agreement on behalf of the Controller represents that they are authorised to represent the Controller.
- (7) The Processor makes the text of this agreement available for retrieval and storage when it is concluded and will provide it to the Controller again in text form at any time on request.

§ 2 Instructions of the Controller

- (1) The Processor processes personal data solely on documented instructions from the Controller, including with regard to transfers to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Art. 28(3)(a) GDPR).
- (2) This agreement including its annexes, together with the Main Agreement, constitutes the Controller's initial instruction. Further instructions shall as a rule be issued by the Controller in text form. Instructions given orally shall be confirmed by the Controller in text form without undue delay.

(3) The persons authorised to issue and to receive instructions are named in Annex 4. Changes shall be notified to the other Party in text form. Notifications by the Processor under this agreement, in particular under §§ 7 and 9, are sent by e-mail to the e-mail address stored in the Controller's customer account. The Controller is responsible for keeping this e-mail address up to date.

(4) If the Processor considers that an instruction infringes data protection law, it shall inform the Controller without undue delay (Art. 28(3) sentence 3 GDPR). The Processor is entitled to suspend the execution of the instruction concerned until it is confirmed or amended by the Controller.

(5) Where the implementation of an instruction goes beyond the services agreed in the Main Agreement and requires substantial additional effort, the Processor may charge reasonable remuneration at its rates applicable from time to time. The Processor shall notify the Controller before performing such work.

§ 3 Obligations of the Controller

(1) As controller, the Controller is solely responsible for the lawfulness of the processing and for safeguarding the rights of data subjects. In particular, the Controller must ensure that a legal basis for the processing exists, that the information obligations under Art. 13 and 14 GDPR are met and that any required consents have been validly obtained.

(2) The Controller undertakes not to enter into the Hub any special categories of personal data within the meaning of Art. 9 GDPR, unless this has been expressly agreed in Annex 1 and secured by appropriate additional protective measures.

(3) The Controller shall inform the Processor without undue delay if it detects errors or irregularities when reviewing the results of the processing.

(4) The Controller is responsible for backing up its own data, unless data backup by the Processor has been agreed in the Main Agreement.

§ 4 Obligations of the Processor

(1) The Processor processes personal data exclusively within the scope of the engagement and the Controller's instructions. No processing for the Processor's own purposes takes place.

(2) The Processor shall organise its internal operations so as to meet the specific requirements of data protection and shall implement the technical and organisational measures set out in § 6 of this agreement.

(3) The Processor confirms that it is aware of and complies with the provisions applicable to processing on behalf of a controller, in particular the GDPR and the German Federal Data Protection Act (BDSG).

(4) The Processor maintains a record of all categories of processing activities carried out on behalf of the Controller pursuant to Art. 30(2) GDPR.

(5) The Processor shall provide the Controller with the contact details of its data protection officer or, where no obligation to designate one exists, of its contact person for data protection matters. The contact person is:

Dr. Colin Reiff, info@collectu.de

(6) If the Processor becomes aware of supervisory authority action relating to the processing carried out for the Controller, it shall inform the Controller without undue delay, to the extent legally permissible.

(7) If the Processor receives a request from an authority or a court for the disclosure of the Controller's personal data, it shall inform the Controller without undue delay to the extent legally permissible, refer the requesting body to the Controller and shall not disclose any data unless legally obliged to do so.

(8) The Processor shall rectify, erase or restrict the processing of data covered by this agreement only on the Controller's instructions.

§ 5 Confidentiality

(1) The Processor ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR).

(2) The confidentiality obligation continues to apply after the end of the employment or contractual relationship and after termination of this agreement.

(3) The Processor ensures that the persons entrusted with the processing are regularly instructed and made aware of data protection requirements.

(4) Access to the Controller's personal data is granted on a need-to-know basis and is logged.

§ 6 Technical and organisational measures

(1) The Processor implements the technical and organisational measures required to ensure a level of security appropriate to the risk pursuant to Art. 32 GDPR. The measures in place at the time this agreement is concluded are described in Annex 2. Where special categories of personal data pursuant to Art. 9 GDPR are processed, the Processor shall additionally implement the appropriate and specific measures required by Section 22(2) BDSG.

(2) The technical and organisational measures are subject to technical progress and further development. The Processor is permitted to implement alternative measures of equivalent

effect. The level of security established in Annex 2 must not be reduced. Material changes shall be documented and communicated to the Controller on request.

§ 7 Sub-processors

(1) The contractually agreed services are performed using the sub-processors listed in Annex 3. The sub-processors engaged at the time this agreement is concluded are listed in Annex 3 and are hereby approved.

(2) The Processor shall inform the Controller in text form of any intended change concerning the addition or replacement of sub-processors with reasonable advance notice before the engagement. The Controller may object to the change in text form within two (2) weeks of receipt of the information on important data protection grounds. If no reasoned objection is raised within this period, the addition or replacement shall be deemed approved.

(3) If the Controller objects and the Processor cannot provide the service concerned without the sub-processor at reasonable expense, either Party is entitled to terminate the Main Agreement extraordinarily with one (1) month's notice. Fees already paid in advance shall be refunded pro rata for the unused period.

(4) The Processor is obliged to select sub-processors carefully on the basis of their suitability and reliability. Where sub-processors in a third country are to be involved, the Processor shall ensure that an adequate level of data protection is guaranteed at the respective sub-processor. On request, the Processor shall provide the Controller with evidence that the aforementioned agreements have been concluded with its sub-processors.

(5) The Processor imposes on the sub-processor, by contract, the same data protection obligations as those set out in this agreement (Art. 28(4) GDPR). Where a sub-processor fails to fulfil its data protection obligations, the Processor remains fully liable to the Controller for the performance of those obligations.

(6) Ancillary services which the Processor obtains from third parties and which are not directed at the processing of the Controller's personal data (e.g. telecommunications services, cleaning, maintenance without access to data) do not constitute sub-processing within the meaning of this provision. The Processor shall nevertheless ensure that data protection and data security are safeguarded in these cases as well.

§ 8 Assistance to the Controller, rights of data subjects

(1) Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as this is possible, in fulfilling its obligation to respond to requests by data subjects exercising their rights under Chapter III GDPR (Art. 28(3)(e) GDPR).

(2) If a data subject contacts the Processor directly, the Processor shall forward the request to the Controller without undue delay and shall not respond to it itself.

(3) The Processor further assists the Controller in complying with the obligations set out in Art. 32 to 36 GDPR, in particular the security of processing, the notification of personal data breaches, data protection impact assessments and prior consultation (Art. 28(3)(f) GDPR), taking into account the nature of the processing and the information available to the Processor.

(4) The Processor may charge reasonable remuneration for assistance that goes beyond the assistance owed by law or that is not attributable to circumstances within the Processor's responsibility.

§ 9 Personal data breaches

(1) The Processor shall notify the Controller in text form, without undue delay, of any personal data breach affecting the Controller's personal data of which it becomes aware.

(2) The notification shall contain, as far as possible, at least the information set out in Art. 33(3) GDPR:

- a description of the nature of the breach including, where possible, the categories and approximate number of data subjects and records concerned;
- the name and contact details of the contact point for further information;
- a description of the likely consequences of the breach;
- a description of the measures taken or proposed to address the breach and to mitigate its possible adverse effects.

(3) The Processor shall take the necessary measures to secure the data and to mitigate possible adverse consequences without undue delay and shall coordinate these measures with the Controller.

(4) Notifications to the supervisory authority under Art. 33 GDPR and communications to data subjects under Art. 34 GDPR are the sole responsibility of the Controller. The Processor does not make such notifications on the Controller's behalf on its own initiative.

§ 10 Evidence and audit rights

(1) The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allows for and contributes to audits conducted by the Controller or another auditor mandated by the Controller (Art. 28(3)(h) GDPR).

(2) Evidence may in particular be provided by:

- adherence to approved codes of conduct pursuant to Art. 40 GDPR;
- certification under an approved certification mechanism pursuant to Art. 42 GDPR;

- current attestations, reports or extracts from reports by independent bodies (e.g. auditors, data protection officers, IT security departments, ISO 27001 certificate, SOC 2 report);
- suitable certification through IT security or data protection audit procedures;
- submission of a current self-assessment or documentation of the technical and organisational measures.

(3) Where the evidence submitted is not sufficient in an individual case, the Controller is entitled, after giving reasonable notice of at least two (2) weeks, to satisfy itself of compliance with this agreement during normal business hours and without disrupting operations. As a rule, the Controller shall carry out on-site audits no more than once per calendar year; where there are specific indications of an infringement, or following a personal data breach, audits may also be carried out on an ad hoc basis and at short notice. On-site audits shall be limited to the extent necessary to verify the processing carried out under this agreement.

(4) The Controller shall ensure that audits are conducted only by persons who are bound by confidentiality and who are not in competition with the Processor. Trade and business secrets of the Processor and the data of other customers must be protected.

(5) The Processor may charge reasonable remuneration for the effort caused by on-site audits, unless the audit is attributable to circumstances within the Processor's responsibility.

§ 11 Deletion and return after termination

(1) After the end of the provision of the processing services, the Processor shall, at the Controller's choice, delete or return all personal data and delete existing copies, unless Union or Member State law requires storage of the personal data (Art. 28(3)(g) GDPR).

(2) The Controller shall communicate its choice in text form no later than the date on which the termination takes effect. If the Controller does not make a choice, the Processor shall make the data available for export in a commonly used, structured and machine-readable format for a period of thirty (30) calendar days from the end of the contract and shall delete them thereafter.

(3) Deletion shall take place no later than ninety (90) calendar days after the end of the contract, including deletion from backup copies within the regular backup cycle. The Processor shall confirm complete deletion in text form on request.

(4) Documentation serving as evidence of processing carried out in accordance with the engagement and with the law may be retained by the Processor beyond the end of the contract in line with the applicable retention periods. The Processor may hand such documentation over to the Controller at the end of the contract in order to discharge itself of the retention obligation.

§ 12 Processing in third countries

(1) Processing of personal data in a third country within the meaning of the GDPR takes place only where the specific requirements of Art. 44 et seq. GDPR are met.

(2) A transfer is permissible in particular on the basis of an adequacy decision of the European Commission (Art. 45 GDPR) or on the basis of the standard contractual clauses adopted by the European Commission (Art. 46(2)(c) GDPR), together with a documented assessment of the effectiveness of the safeguards in the recipient country (transfer impact assessment) and, where necessary, supplementary protective measures.

(3) Remote access to personal data from a third country, in particular in the course of support or maintenance services, constitutes a transfer within the meaning of this provision.

§ 13 Liability

(1) The liability of the Parties towards each other is governed by the provisions of the Main Agreement, unless otherwise stipulated in this agreement.

(2) In relation to data subjects, Art. 82 GDPR applies.

(3) As between themselves, the Parties shall indemnify each other against claims by data subjects and against administrative fines in accordance with their respective share of responsibility.

§ 14 Final provisions

(1) This agreement takes precedence over the provisions of the Main Agreement, including the Processor's General Terms and Conditions, insofar as it concerns the processing of personal data on behalf of the Controller. In all other respects, the provisions of the Main Agreement apply.

(2) Amendments and additions to this agreement and its annexes must be made in text form. This also applies to any waiver of this form requirement.

(3) Should individual provisions of this agreement be or become invalid or unenforceable, the validity of the remaining provisions shall remain unaffected. The Parties undertake to replace the invalid or unenforceable provision with a valid provision that comes closest to the economic purpose of the replaced provision.

(4) This agreement is governed by the laws of the Federal Republic of Germany. The place of jurisdiction is Stuttgart, to the extent legally permissible.

(5) Annexes 1 to 4 form an integral part of this agreement.

(6) This agreement is available in German and English. In the event of discrepancies, the German version prevails.

This agreement is concluded electronically (§ 1(5)) and is effective without signature.

Annex 1

Description of the processing

1. Subject matter of the processing

Provision and operation of the software "Collectu" for the collection, transmission, storage, processing and analysis of data from the Controller's systems, together with the associated support, maintenance and operating services.

2. Nature and purpose of the processing

- provision, operation and maintenance of the Hub and of the Core installed at the Controller's premises
- administration of the Controller's user accounts, roles and permissions
- storage and processing of the data entered by the Controller ("user data")
- generation of analyses, visualisations and reports within the Hub
- processing by AI-supported functions of the Hub, where activated by the Controller
- logging to ensure system security and the traceability of access
- data backup and restoration
- error analysis, support and – subject to the Controller's prior consent – temporary remote access pursuant to clause 12.5 of the General Terms and Conditions

3. Types of personal data

The processing covers the following types of data:

Category	Examples
Master and contact data of the Controller's users	surname, first name, business e-mail address, user name, organisational unit, role
Contract and billing data	company name, billing address, plan booked, payment data (where collected)
Usage and log data	timestamps, IP address, device and browser information, functions accessed, configuration changes, error and security logs
Authentication data	password hashes, tokens, API keys, session information
Communication and support data	content of support requests, e-mail correspondence, error descriptions and log files submitted

Category	Examples
Content data entered by the Controller	process, machine and sensor data recorded from the Controller's systems and other content, insofar as such data relate to an identifiable person (e.g. operator or shift identifiers, links to work orders or time recording). The scope and any personal reference are determined solely by the Controller.

Special categories of personal data under Art. 9 GDPR are not the subject of the processing unless otherwise agreed.

4. Categories of data subjects

- employees of the Controller (in particular users, administrators, contact persons)
- employees of affiliated companies and external service providers of the Controller, insofar as they are granted access
- customers, suppliers and other business partners of the Controller, insofar as their data are entered by the Controller
- other natural persons whose data the Controller enters into the Hub

5. Duration of the processing

Processing takes place for the term of the Main Agreement. After its termination, § 11 of this agreement applies.

6. Place of processing

Data centre locations within the Federal Republic of Germany. Administration of the systems is carried out from the Processor's registered office in Stuttgart.

Annex 2

Technical and organisational measures pursuant to Article 32 GDPR

1. Confidentiality (Art. 32(1)(b) GDPR)

Physical access control

- servers are operated exclusively in certified data centres of the service providers listed in Annex 3, with access control systems, video surveillance, alarm systems and documented visitor management
- Processor's own premises: locking system with documented key allocation; visitors are accompanied

System access control

- personal, non-shared user accounts for all systems
- password policy with minimum length, complexity requirements and lockout after failed attempts
- passwords stored exclusively as salted hashes
- multi-factor authentication where activated by the Controller
- automatic locking of inactive sessions
- administrative access to the production environment exclusively via encrypted connections and from defined network ranges

Data access control

- role and permission concept based on the principle of least privilege
- tenant separation: logical separation of the data of different controllers
- logging of administrative access to production data
- defined procedure for granting, changing and withdrawing permissions, in particular when employees leave
- data carriers are securely erased or destroyed before disposal (DIN 66399)

Separation control

- logical separation of production, test and development environments
- no use of production data in test and development environments

Pseudonymisation and encryption

- transport encryption of all connections (TLS 1.2 or higher)
- encryption of data at rest on storage media and in backups
- full disk encryption on employee devices
- pseudonymisation where the purpose of the processing permits

2. Integrity (Art. 32(1)(b) GDPR)

Transfer control

- transmission between the Core and the Hub exclusively encrypted and authenticated
- no transfer of personal data to third parties other than the sub-processors listed in Annex 3
- documentation of data flows

Input control

- logging of security-relevant events and of changes to configurations and permissions
- traceability of which user account made which change
- tamper-resistant retention of log data for a defined period

3. Availability and resilience (Art. 32(1)(b) and (c) GDPR)

- redundant data centre infrastructure (power, cooling, network connectivity, fire protection)
- regular, automated data backups with defined retention periods
- backups stored separately from the production systems
- regular testing of the restorability of backups
- firewalls, network segmentation and protection against denial-of-service attacks
- monitoring and alerting for system faults
- timely installation of security-relevant updates (patch management)
- documented business continuity and disaster recovery plan with defined recovery objectives

4. Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR)

- data protection management with documented internal policies
- record of categories of processing activities pursuant to Art. 30(2) GDPR
- commitment of all employees to confidentiality and regular data protection and IT security training
- documented process for detecting, assessing and reporting personal data breaches
- documented process for handling data subject requests
- supplier control: selection and regular review of sub-processors, conclusion of agreements pursuant to Art. 28 GDPR
- data protection by design and by default (Art. 25 GDPR)
- regular review of the technical and organisational measures, at least annually
- security review of source code and dependencies within the development process

Annex 3

Approved sub-processors

Company, address	Service	Place of processing
IONOS SE Elgendorfer Str. 57 56410 Montabaur, Germany	Hosting and operation of the server and storage infrastructure of the Hub, including backups	Germany, EU
OpenAI Ireland Limited 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	Provision of AI models for the AI-supported functions of the Hub	Ireland and USA transfer on the basis of the EU Standard Contractual Clauses (Art. 46(2)(c) GDPR)

Changes are notified in accordance with § 7 of this agreement.

Annex 4

Contact persons and persons authorised to issue instructions

	Controller	Processor
Person(s) authorised to issue instructions	Users with owner or administrator rights in the Controller's customer account	Name: Dr. Colin Reiff Role: Managing Director E-mail: colin.reiff@collectu.de Name: Dr. Frederik Wulle Role: Managing Director E-mail: frederik.wulle@collectu.de
Person(s) authorised to receive instructions	Not applicable	Designated employees of the Processor in accordance with internal policies on areas of responsibility
Data protection officer or data protection contact	The Controller's data protection officer, if notified to the Processor; otherwise the e-mail address stored in the customer account	Name: Dr. Colin Reiff E-mail: info@collectu.de
Contact point for security incidents	The e-mail address stored in the customer account	E-mail: security@collectu.de

The Controller may notify different or additional contact persons, as well as its data protection officer, at any time in text form to info@collectu.de.