cedalo

Data Processing Agreement

Version 2.0, published 19.11.2026 at https://cedalo.com/dpa

between

the customer named in the Main Contract

as Controller (hereinafter "**Controller**"),

and

Cedalo GmbH, Schnewlinstraße 6, 79098 Freiburg, Germany

as Data Processor (hereinafter "**Data Processor**",

Controller and Data Processor jointly the "**Parties**")

Preamble

The Controller has commissioned the Data Processor in a contract already concluded (hereinafter referred to as the "**Main Contract**") for the services specified therein. Part of the execution of the contract is the processing of personal data. In particular, Art. 28 GDPR imposes specific requirements on such commissioned processing. To comply with these requirements, the following Data Processing Agreement (hereinafter referred to as the "**Agreement**") applies between the Parties, the performance of which shall not be remunerated separately unless expressly agreed.

Where the Main Contract or the Data Processor's Terms and Conditions of Business refer to this Agreement, this Agreement forms part of the Main Contract upon its conclusion and applies to the extent that the Data Processor processes personal data on behalf of the Controller. No separate signature is required. An individually negotiated data processing agreement between the Parties shall take precedence over this Agreement.

§ 1 Definitions

(1) Pursuant to Art. 4 (7) GDPR, the Controller is the entity that alone or jointly with other Controllers determines the purposes and means of the processing of personal data.

(2) Pursuant to Art. 4 (8) GDPR, a Data Processor is a natural or legal person, authority, institution, or other body that processes personal data on behalf of the Controller.

(3) Pursuant to Art. 4 (1) GDPR, personal data means any information relating to an identified or identifiable natural person (hereinafter "**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(4) Personal data requiring special protection are personal data pursuant to Art. 9 GDPR revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of Data Subjects, personal data pursuant to Art. 10 GDPR on criminal convictions and criminal offenses or related security measures, as well as genetic data pursuant to Art. 4 (13) GDPR, biometric data pursuant to Art. 4 (14) GDPR, health data pursuant to Art. 4 (15) GDPR, and data on the sex life or sexual orientation of a natural person.

(5) According to Article 4 (2) GDPR, the processing is any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(6) Pursuant to Article 4 (21) GDPR, the supervisory authority is an independent state body established by a Member State pursuant to Article 51 GDPR.

§ 2 Subject of the contract

(1) The Data Processor provides the services specified in the Main Contract for the Controller. In doing so, the Data Processor obtains access to personal data, which the Data Processor processes for the Controller exclusively on behalf of and in accordance with the Controller's instructions. The scope and purpose of the data processing by the Data Processor are set out in the Main Contract and any associated service descriptions. The Controller shall be responsible for assessing the admissibility of the data processing.

(2) This Agreement specifies the mutual rights and obligations of the Parties under data protection law. Unless otherwise provided in this Agreement, the provisions of this Agreement shall take precedence over the provisions of the Main Contract in case of doubt.

(3) The provisions of this contract shall apply to all activities related to the Main Contract in which the Data Processor and its employees or persons authorized by the Data Processor come into contact with personal data originating from the Controller or collected for the Controller.

(4) The term of this Agreement shall be governed by the term of the Main Contract unless the following provisions give rise to further obligations or termination rights.

§ 3 Right of instruction

(1) The Data Processor may only collect, process or use data within the scope of the Main Contract and in accordance with the instructions of the Controller. If the Data Processor is required to carry out further processing by the law of the European Union or the Member States to which it is subject, it shall notify the Controller of these legal requirements prior to the processing.

(2) The instructions of the Controller shall initially be determined by this Agreement. Thereafter, they may be amended, supplemented, or replaced by the Controller in writing or text form by individual instructions (Individual Instructions). The Controller shall be entitled to issue such instructions at any time. This includes instructions with regard to the correction, deletion, and blocking of data.

(3) All instructions issued shall be documented by the Controller. Instructions that go beyond the service agreed in the Main Contract shall be treated as a request for a change in service.

(4) If the Data Processor is of the opinion that an instruction of the Controller violates data protection provisions, it shall notify the Controller thereof without undue delay. The Data Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller. The Data Processor may refuse to carry out an obviously unlawful instruction.

§ 4 Types of data processed, group of Data Subjects, third country

(1) Within the scope of the implementation of the Main Contract, the Data Processor shall have access to the personal data specified in more detail in **Annex 1**.

(2) The group of Data Subjects affected by the data processing is listed in **Annex 2**.

(3) A transfer of personal data to a third country may take place under the conditions of Art. 44 et seq. GDPR.

(4) The data-centre location of a Cedalo Cloud instance is selected by the Controller when the instance is set up. If the Controller selects a location in the European Union, personal data is processed exclusively in the European Union. If the Controller selects a location in the United States, personal data is processed in the United States by the Sub-processors designated accordingly in the Sub-processor List; this selection constitutes the Controller's documented instruction within the meaning of Art. 28(3)(a) GDPR. Transfers to Hetzner US LLC are based on the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914, Module 3) concluded between Hetzner Online GmbH and Hetzner US LLC. Where the Controller's own contractual or regulatory requirements exclude processing outside the European Union, the Controller shall select an EU location.

§ 5 Protective measures of the Data Processor

(1) The Data Processor shall be obliged to observe the statutory provisions on data protection and not to disclose information obtained from the Controller's domain to third parties or expose it to their access. Documents and data shall be secured against disclosure to unauthorized persons, taking into account the state of the art.

(2) The Data Processor shall organize the internal organization within its field of responsibility in such a way that it meets the special requirements of data protection. It shall have taken the technical and organizational measures specified in **Annex 3** to adequately protect the Controller's data pursuant to Art. 32 GDPR, which the Controller acknowledges as adequate. The Data Processor reserves the right to change the security measures taken while ensuring that the contractually agreed level of protection is not undercut.

(3) The persons employed in the data processing by the Data Processor are prohibited from collecting, processing or using personal data without authorization. The Data Processor shall oblige all persons entrusted by it with the processing and performance of this contract (hereinafter "**Employees**") accordingly (obligation of confidentiality, Art. 28 (3) lit. b GDPR) and shall ensure compliance with this obligation with due care.

(4) The Data Processor has appointed a data protection officer. The Data Processor's data protection officer is heyData GmbH, Bertolt-Brecht-Platz 3, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Information obligations of the Data Processor

(1) If the Data Processor becomes aware of a personal data breach or a suspected personal data breach affecting the Controller's personal data, or of a breach of this Agreement or of data protection provisions in the processing of the Controller's personal data by the Data Processor, persons employed by it or its Sub-processors, the Data Processor shall inform the Controller without undue delay. The same shall apply to inspections or other measures of a data protection supervisory authority insofar as they concern the processing of the Controller's personal data. The notification of a personal data breach shall contain at least the following information:

(a) a description of the nature of the personal data breach, including, to the extent possible, the categories and the number of Data Subjects affected, the categories affected and the number of personal data records affected;

(b) a description of the measures taken or proposed by the Data Processor to address the breach and, where applicable, measures to mitigate its possible adverse effects;

(c) a description of the likely consequences of the personal data breach.

(2) The Data Processor shall immediately take the necessary measures to secure the data and to mitigate any possible adverse consequences for the Data Subjects, inform the Controller thereof and request further instructions.

(3) In addition, the Data Processor shall be obliged to provide the Controller with information at any time insofar as the Controller's data are affected by a breach pursuant to paragraph 1.

(4) The Data Processor shall inform the Controller of any significant changes to the security measures pursuant to Section 5 (2).

§ 7 Control rights of the Controller

(1) The Controller may satisfy itself of the technical and organizational measures of the Data Processor prior to the commencement of data processing and thereafter regularly on a yearly basis. For this purpose, the Controller shall primarily rely on current certificates and audit reports provided by the Data Processor (in particular its ISO/IEC 27001 certification and SOC 2 report) and on information provided by the Data Processor. An on-

site inspection by the Controller or by a competent third party bound to confidentiality and not in a competitive relationship with the Data Processor is permitted only if such evidence is insufficient in the individual case or if there is a specific reason (in particular a personal data breach), with at least 30 days' prior notice, during normal business hours and at the Controller's expense. The Controller shall carry out checks only to the extent necessary and shall not disproportionately disrupt the operations of the Data Processor in the process.

(2) The Data Processor undertakes to provide the Controller, upon the latter's verbal or written request and within a reasonable period of time, with all information and evidence required to carry out a check of the technical and organizational measures of the Data Processor.

(3) The Controller shall document the results of the inspection and notify the Data Processor thereof. In the event of errors or irregularities which the Controller discovers, in particular during the inspection of the results of the inspection, the Controller shall inform the Data Processor without undue delay. If facts are found during the control, the future avoidance of which requires changes to the ordered procedure, the Controller shall notify the Data Processor of the necessary procedural changes without delay.

§ 8 Use of service providers

(1) The contractually agreed services shall be performed with the involvement of the service providers listed in the list of sub-processors published at https://cedalo.com/subprocessors (hereinafter "Sub-processors" and "Sub-processor List"). The Sub-processor List forms part of this Agreement. The Controller grants the Data Processor its general authorization within the meaning of Article 28 (2) s. 1 GDPR to engage additional Sub-processors within the scope of its contractual obligations or to replace Sub-processors already engaged.

(2) The Data Processor shall inform the Controller of any intended addition or replacement of a Sub-processor at least 14 days in advance by e-mail to the notification address provided by the Controller (or, if none has been provided, to the Controller's contact address known to the Data Processor) and by updating the Sub-processor List. In addition, the Controller may subscribe to change notifications by sending an e-mail with the subject "Subscribe" to privacy@cedalo.com. The Controller may object to an intended addition or replacement of a Sub-processor for good cause under data protection law.

(3) The objection must be raised in text form to privacy@cedalo.com within 14 days of receipt of the information pursuant to paragraph 2. If no objection is raised within this period, the addition or replacement shall be deemed approved. If there is good cause under data protection law and no mutually agreeable solution can be found between the

Controller and the Data Processor, the Controller shall have a special right to terminate the affected services at the end of the month following the objection.

(4) Where the immediate replacement of a Sub-processor is required for reasons beyond the Data Processor's control (in particular security reasons, insolvency or discontinuation of the service by the Sub-processor), the Data Processor may carry out the replacement without prior notice and shall inform the Controller without undue delay; paragraph 3 shall apply accordingly from receipt of this information.

(5) When engaging Sub-processors, the Data Processor shall oblige them in accordance with the provisions of this Agreement.

(6) Sub-processors may engage further sub-processors in accordance with their own data processing terms; these are listed in the respective Sub-processor's published list referenced in the Sub-processor List. The general authorization pursuant to paragraph 1 extends to such further sub-processors. The notification obligation pursuant to paragraph 2 applies to Sub-processors engaged directly by the Data Processor. Where the Data Processor becomes aware of a change of such further sub-processors that results in the Controller's personal data actually being processed in a third country not previously covered by the Sub-processor List, it shall inform the Controller without undue delay; paragraph 3 shall apply accordingly.

(7) A Sub-processor relationship within the meaning of these provisions does not exist if the Data Processor commissions third parties with services that are regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific reference to services provided by the Data Processor to the Controller and guarding services. Maintenance and testing services constitute Sub-processor relationships within the meaning of this § 8 insofar as they are provided for IT systems that are also used in connection with the provision of services for the Controller.

§ 9 Requests and rights of Data Subjects

(1) The Data Processor shall support the Controller with suitable technical and organizational measures in fulfilling the Controller's obligations pursuant to Articles 12-22 and 32 to 36 GDPR.

(2) If a Data Subject asserts rights, such as the right of access, correction or deletion with regard to his or her data, directly against the Data Processor, the latter shall not react independently but shall refer the Data Subject to the Controller and await the Controller's instructions.

§ 10 Liability

(1) The Parties shall be liable to Data Subjects in accordance with Art. 82 GDPR. The Data Processor shall be liable for damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Controller (Art. 82 (2) GDPR). In the relationship between the Parties, including recourse pursuant to Art. 82 (5) GDPR, the liability provisions of the Main Contract shall apply.

§ 11 Termination of the Main Contract

(1) After termination of the Main Contract, the Data Processor shall return to the Controller all documents, data and data carriers provided to it or - at the request of the Controller, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany - delete them. This shall also apply to data backups at the Data Processor and its Sub-processors; backups shall be deleted in the regular backup cycle, at the latest 30 days after termination of the Main Contract. The Data Processor shall on request provide documented proof of the proper deletion of any data.

(2) The Controller shall have the right to control the complete and contractual return or deletion of the data at the Data Processor in an appropriate manner.

(3) The Data Processor shall be obligated to keep confidential the data of which it has become aware in connection with the Main Contract even beyond the end of the Main Contract. The present Agreement shall remain valid beyond the end of the Main Contract as long as the Data Processor has personal data at its disposal which have been forwarded to it by the Controller or which it has collected for the Controller.

§ 12 Final provisions

(1) To the extent that the Data Processor does not expressly perform support actions under this Agreement free of charge, it may charge the Controller a reasonable fee therefore, unless the Data Processor's own actions or omissions have made such support directly necessary.

(2) Amendments to this Agreement shall be notified to the Controller in accordance with the amendment provisions of the Main Contract or the Data Processor’s Terms and Conditions of Business; changes of Sub-processors are governed exclusively by § 8.

Amendments individually agreed between the Parties require text form. The priority of individual contractual agreements shall remain unaffected.

(3) If individual provisions of this Agreement are or become wholly or partially invalid or unenforceable, this shall not affect the validity of the remaining provisions.

(4) This Agreement is subject to German law. Unless the Main Contract provides otherwise, the exclusive place of jurisdiction for all disputes arising from or in connection with this Agreement is Freiburg im Breisgau, Germany, provided that the Controller is a merchant, a legal entity under public law or has no general place of jurisdiction in Germany.

Signature is optional. Where this Agreement is incorporated into the Main Contract by reference (see Preamble), no signature is required. Upon request, the Data Processor will provide a signed copy.

Controller

Name: _____

Position: _____

Date: _____

Signature: _____

Data Processor

Name: Philipp Struß

Position: CEO

Date: _____

Signature: _____

Annex

Annex 1 - Description of the data/data categories

E-mail address, IP addresses, client ID, username and password, log data, other device data inserted by the customer themselves; content of messages transmitted via the broker, to the extent that it contains personal data (as determined by the Controller)

Annex 2 - Description of affected Data Subject/groups of affected Data Subjects

Employees of the controller, customers of the controller, other third parties

Annex 3 - Technical and organizational measures of the Data Processor

1. Introduction

1.1 Subject of the document

This document summarises the technical and organisational measures taken within the meaning of Art. 32 (1) GDPR.

2. Confidentiality (Art. 32 para. 1 lit. b GDPR)

2.1 Physical access control

The following implemented measures prevent unauthorised persons from gaining access to the data processing systems:

- Manual locking system (e.g. key)
- Visitors must be accompanied by employees

- Instructions to employees not to work in publicly accessible areas (e.g. cafés)
- Working from home: unauthorised persons have no access to employees' homes

2.2 System access control

The following implemented measures prevent unauthorised persons from gaining access to the data processing systems:

- Management of user authorisations
- Multi-factor authentication for access to administrative and production systems

2.3 Data access control

The following implemented measures ensure that unauthorised persons have no access to personal data:

- Management of user rights by system administrators

2.4 Separation control

The following measures ensure that personal data collected for different purposes is processed separately:

- Separation of production and test system
- Encryption of data records that are processed for the same purpose
- Logical client separation (on the software side)
- For pseudonymised data: Separate storage of the allocation file on a separate, secure IT system (encrypted if possible)
- Definition of database rights
- Internal instruction to anonymise/pseudonymise personal data in the event of disclosure or after expiry of the statutory deletion period, if possible.

3. Integrity (Art. 32 para. 1 lit. b GDPR)

3.1 Transfer control

It is ensured that personal data cannot be read, copied, changed or removed without authorisation during transmission or storage on data carriers and that it is possible to check which persons or bodies have received personal data. The following measures have been implemented to ensure this:

- Provision of data via encrypted connections such as SFTP or HTTPS
- Encryption of personal data at rest

3.2 Input control

The following measures ensure that it is possible to check who has processed personal data in data processing systems and at what time:

- Logging the entry, modification and deletion of data
- Traceability of data entry, modification and deletion through individual user names (not user groups)
- Assignment of rights to enter, change and delete data on the basis of an authorisation concept
- Clear responsibilities for cancellations
- Instruction to employees to delete data only after consultation

4. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Hosting (at least of the most important data) with a professional hoster
- Hosting in data centres certified according to ISO/IEC 27001
- Regular backups with documented and tested restore procedures
- Offsite backups of Cedalo Cloud instances in a separate data centre in the European Union (from 4 Dec 2026)

5. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

5.1 Data protection management

The following measures are intended to ensure that the organisation meets the basic requirements of data protection law:

- Use of the heyData platform for data protection management
- Appointment of the data protection officer heyData
- Obligation of employees to maintain data secrecy
- Regular data protection training for employees
- Maintaining an overview of processing activities (Art. 30 GDPR)
- Information security management system certified according to ISO/IEC 27001; SOC 2 Type 2 report
- Annual acknowledgement of all information security policies by all employees
- Regular penetration tests

5.2 Incident response management

The following measures are intended to ensure that reporting processes are triggered in the event of data protection violations:

- Reporting process for data protection violations in accordance with Art. 4 (12) GDPR to the supervisory authorities (Art. 33 GDPR)
- Notification process for data breaches in accordance with Art. 4 (12) GDPR to the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches
- Documented incident management procedure with a central reporting address (security@cedalo.com)

5.3 Data protection-friendly default settings (Art. 25 para. 2 GDPR)

The following implemented measures take into account the requirements of the principles of "privacy by design" and "privacy by default":

- Training of employees in "privacy by design" and "privacy by default"
- No more personal data is collected than is necessary for the respective purpose.

5.4 Order control

The following measures ensure that personal data can only be processed in accordance with the instructions:

- Written instructions to the contractor or instructions in text form (e.g. through an order processing contract)
- Ensuring the destruction of data after completion of the order, e.g. by requesting corresponding confirmations
- Confirmation from contractors that they commit their own employees to data secrecy (typically in the order processing contract)
- Careful selection of contractors (especially with regard to data security)

Annex 4 – Sub-processors

The current list of Sub-processors, including their function and processing locations, is published at https://cedalo.com/subprocessors and forms part of this Agreement pursuant to § 8 (1).