

Data Processing Agreement

pursuant to Art. 28 GDPR

As of: October 2026 · replaces the Data Processor Agreement of 10.01.2023 · Convenience translation – the German version is binding

between the Customer as controller (the “Client”)

and Founders1 GmbH, registered office Berlin (Amtsgericht Charlottenburg, HRB 234373 B), business address Berger Straße 224, 60385 Frankfurt am Main, as processor (the “Contractor”).

Preamble

- A.** This Data Processing Agreement (“DPA”) forms part of the agreement on the use of the BetterCo platform, consisting of the Order Form and the Terms of Use (the “Main Agreement”). It is concluded in text form together with the Main Agreement and terminates with it.
- B.** The terms “personal data”, “processing”, “data subject” and “personal data breach” have the meaning given in Regulation (EU) 2016/679 (“GDPR”).
- C.** “Client Matter Data” means the personal data that the Client processes when using the platform in relation to its clients, mandators or customers and the persons associated with them, including identification data, identity documents, ownership structures, screening results and risk assessments. “Professional secrecy” means the obligations under § 203 StGB (German Criminal Code) and the rules of professional law, in particular § 43e BRAO (Federal Lawyers' Act), § 26a BNotO (Federal Notaries Act), § 62a StBerG (Tax Advisers Act) and § 50a WPO (Public Accountants Act).
- D.** The Contractor is itself the controller for the processing of account and billing data, support correspondence and technical operating logs; such processing is not subject to this DPA.

1 Subject matter, duration, nature and purpose

- 1.1** The Contractor processes personal data solely in order to provide the services described in the Main Agreement. The subject matter, duration, nature and purpose of the processing, the type of personal data and the categories of data subjects are set out in Annex 3.
- 1.2** Where the Contractor is required to carry out processing under Union or Member State law, it shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2 Instructions

- 2.1** The Contractor processes personal data only on documented instructions from the Client, including with regard to transfers to a third country. The Main Agreement, including the use of the platform by the Client and its Users, constitutes an instruction. Individual instructions are given in text form.
- 2.2** If the Contractor considers that an instruction infringes data protection provisions, it shall inform the Client without undue delay. It may suspend execution until the matter is clarified.
- 2.3** The Contractor does not process the data for its own purposes and, in particular, does not use it to train artificial intelligence models.
- 2.4** The Contractor maintains a record of processing activities pursuant to Art. 30(2) GDPR.

3 Confidentiality

- 3.1** The Contractor deploys only persons who are bound by confidentiality; this obligation continues after the end of their engagement. Clause 13 applies additionally to Client Matter Data.
- 3.2** If an authority or court requests the disclosure of the Client's data, the Contractor shall notify the Client in advance, insofar as legally permissible. If the order originates from a body outside the European Union, the Contractor shall refer to Art. 48 GDPR and disclose data only insofar as there is a legal basis under Union law.

4 Technical and Organisational Measures

- 4.1** The Contractor implements the measures pursuant to Art. 32 GDPR described in Annex 1. Annex 1 forms part of this DPA.
- 4.2** The Contractor may further develop the measures. The level of protection of Annex 1 must not be undercut in doing so. The Contractor shall notify the Client of material changes in advance in text form.
- 4.3** The Contractor reviews the effectiveness of the measures at least annually and documents the result.

5 Personal data breaches

- 5.1** The Contractor shall notify the Client of any personal data breach affecting the Client's data without undue delay and at the latest within 48 hours after becoming aware of it.
- 5.2** The notification shall contain, insofar as known, the nature of the breach including the categories and approximate number of data subjects and records concerned, a contact point, the likely consequences and the measures taken or proposed. If the breach concerns Client Matter Data, the notification shall state this expressly. Information not immediately available shall be provided subsequently without undue delay.
- 5.3** The Contractor documents every breach and assists the Client with its notification and communication obligations under Art. 33 and 34 GDPR.

6 Locations of processing

- 6.1** The Contractor stores and processes the Client's data, including backups, exclusively within the European Economic Area; this also applies to disaster recovery. The sole exception is support access under clause 6.2. Annex 2 specifies the locations for each service.
- 6.2** Microsoft and MongoDB have no standing access to the data. Access by their personnel is technically blocked (Customer Lockbox for Microsoft Azure, blocking of support access in MongoDB Atlas) and is possible only in critical incidents affecting operations or security, following prior approval by the Contractor in each individual case and for a limited period. Where such access takes place from a third country, it is based on the EU-US Data Privacy Framework (Art. 45 GDPR) or the Standard Contractual Clauses (Art. 46 GDPR) in the agreements with the providers. The Contractor logs every approval and makes the assessment of such access (Transfer Impact Assessment) available to the Client on request.
- 6.3** Any further transfer to a third country requires an instruction from the Client in text form and compliance with Chapter V GDPR.

7 Sub-processors

- 7.1** The Client approves the engagement of the sub-processors listed in Annex 2. Annex 2 is also published at betterco.ai/subprocessors.
- 7.2** The Contractor shall inform the Client in text form at least 30 days in advance of any intended addition or replacement of a sub-processor. The Client may object in text form within 30 days of receipt on objective grounds, in particular for reasons of data protection or professional secrecy. Until an agreement is reached, the Contractor shall not use the new sub-processor for the data of the objecting Client. If this is not possible, or if no agreement is reached within 30 days of the objection, the Client may terminate this DPA and the Main Agreement with effect from the date of deployment; fees paid in advance for the period thereafter shall be refunded pro rata.
- 7.3** The Contractor contractually imposes on each sub-processor the same data protection obligations as apply to the Contractor under this DPA and remains fully liable to the Client for the sub-processor's compliance. If a sub-processor receives Client Matter Data, the Contractor shall additionally bind it in accordance with clause 13.
- 7.4** Ancillary services in which the service provider obtains no access to the Client's data, such as telecommunications services, do not constitute sub-processing.

8 Rights of data subjects

- 8.1** The Contractor assists the Client by appropriate technical and organisational measures in fulfilling the rights of data subjects under Chapter III GDPR, in particular access, rectification, restriction, erasure and data portability.
- 8.2** If a data subject contacts the Contractor directly, the Contractor shall forward the request to the Client without undue delay and shall not respond to it itself.

9 Assistance, evidence and audits

- 9.1** The Contractor assists the Client in complying with the obligations under Art. 32 to 36 GDPR, including data protection impact assessments and prior consultations.
- 9.2** The Contractor makes available to the Client all information necessary to demonstrate compliance with this DPA. As it currently holds no certification of its own, it provides for this purpose in particular Annex 1, the result of the annual effectiveness review and the certifications of its sub-processors.
- 9.3** The Client, or an auditor mandated by it and bound by confidentiality, may conduct audits, including inspections. Regular audits shall be announced at least 30 days in advance, take place during normal business hours and no more than once per contract year. For Microsoft and MongoDB, evidence is provided by way of their certifications and audit reports under clause 9.2; inspections of their data centres are excluded.
- 9.4** The Client may audit without notice period and without counting towards clause 9.3 if a personal data breach has been notified, a supervisory authority or professional body so requires, a sub-processor for Client Matter Data is changed, or there are specific indications of a breach of this DPA.
- 9.5** Audits shall be conducted with due regard to the Contractor's business operations and the confidentiality of other customers' data.

10 Obligations of the Client

- 10.1** The Client is responsible for the lawfulness of the processing, in particular for the legal bases, including those under Art. 9 and 10 GDPR, and for informing the data subjects. It shall inform the Contractor without undue delay if it detects errors or irregularities in the processing.

11 Erasure and return

- 11.1** Upon termination of the Main Agreement, the Contractor shall erase the Client's data or, at the Client's option, return it. The Client shall communicate its choice within 30 days of the end of the agreement; if it makes no choice, the data will be erased. Before erasure, the Contractor shall draw attention to the option of export.
- 11.2** Erasure or return takes place within 30 days of receipt of the choice or expiry of the period for making it. The Contractor confirms erasure in text form with an erasure log stating the date, scope and systems concerned.
- 11.3** Data in backups is removed in the regular backup rotation, at the latest after 12 months, and is not restored to production until then.
- 11.4** Longer retention takes place only insofar as required by Union or Member State law; the Contractor shall state the legal basis and duration.

12 Processing using artificial intelligence

- 12.1** The Contractor uses a language model to extract information from uploaded documents and pre-fill details. Processing takes place exclusively via the Azure OpenAI Service listed in Annex 2, in a deployment restricted to the EU Data Zone.
- 12.2** Input and output data are not used to train or improve models.
- 12.3** Outputs are labelled suggestions that are adopted only after confirmation or correction by a human. Decisions, in particular under the GwG (German Anti-Money Laundering Act), are taken by the Client.
- 12.4** The use of any further AI service constitutes a change of sub-processors under clause 7.

13 Professional secrecy

- 13.1** Insofar as the Client is a professional secrecy holder or processes data subject to professional secrecy, the Contractor is a contributing person within the meaning of § 203(3) StGB. The Professional Secrecy Agreement applies in addition.
- 13.2** The Contractor is obliged to bind all persons who obtain access to Client Matter Data to confidentiality in text form before they commence their activity and to instruct them on criminal liability under §§ 203, 204 StGB. It shall bind sub-processors that receive Client Matter Data in the same way, including the obligation to bind their own subcontractors. All sub-processors receiving Client Matter Data are bound accordingly. Microsoft and MongoDB are exempt, as they do not offer a separate undertaking under § 203 StGB; they provide infrastructure, are bound to confidentiality under their data processing terms and obtain access only in accordance with clause 6.2.
- 13.3** The Contractor restricts access to Client Matter Data to what is necessary for the service, logs access and maintains a register of the undertakings, the current status of which it discloses to the Client on request.

14 Liability

- 14.1** The provisions of the Main Agreement govern the liability of the parties towards each other. Liability towards data subjects under Art. 82 GDPR remains unaffected.

15 Final provisions

- 15.1** In the event of conflicts between this DPA and the Main Agreement, this DPA prevails in matters of data protection.
- 15.2** Amendments to this DPA require text form. The Contractor may amend the DPA with effect for the future insofar as this is necessary due to a change in the legal situation and the level of protection is not reduced; the amendment procedure of the Terms of Use applies mutatis mutandis. Changes of sub-processors are governed exclusively by clause 7.
- 15.3** If the Client's data held by the Contractor is jeopardised by attachment, seizure, insolvency proceedings or other measures by third parties, the Contractor shall notify the Client without undue delay.
- 15.4** German law applies. The place of jurisdiction is Berlin, unless the Main Agreement provides otherwise. The German version is binding.
- 15.5** The invalidity of individual provisions does not affect the validity of the remaining provisions.

Annexes

Annex	Content	Location
Annex 1	Technical and Organisational Measures	betterco.ai/technische-und-organisatorische-massnahmen
Annex 2	Sub-processors and locations of processing	betterco.ai/subprocessors
Annex 3	Subject matter and scope of processing	in this document

Annex 3 – Subject matter and scope of processing

1 Subject matter and duration

The subject matter is the provision and operation of the BetterCo platform as a service over the internet, including the interfaces and the data packages booked by the Client. The platform supports the Client in identifying contracting parties and in fulfilling its due diligence obligations under the GwG and, where applicable, under professional law requirements. Processing lasts for the term of the Main Agreement; return and erasure are governed by clause 11 of the DPA. The Client fulfils its own retention obligations, in particular under § 8(4) GwG, on its own responsibility.

2 Nature and purpose of processing

Module	Nature of processing	Purpose
Onboarding: self-disclosure, conflict and compliance check, creation of clients, opening of files	Collection, structuring, storage, display	Identification of the contracting party and the beneficial owners; documentation of the client relationship
Powers of attorney, consents, resolutions	Collection, storage, provision for signature	Documentation of representation and consent relationships
Risk management	Analysis, assessment, consolidation	Risk classification and ongoing monitoring
Identity verification and signature, including video identification	Collection, matching including biometric facial comparison, storage of the result	Establishment and verification of identity
Data packages Master Data and Master Data GwG	Retrieval from public registers, pre-filling, monitoring for changes; determination of the ownership structure	Accuracy of the information; obligations under §§ 10 et seq. GwG
Data package Compliance	Screening against sanctions, PEP and adverse media lists, one-off or ongoing	Sanctions and reputation check
Extraction of information from documents using a language model	Extraction of information from uploaded documents; suggestions with source references; medical documents are only recognised as such and their content is not analysed	Pre-filling; adoption only after review by a human
Operations, security, support	Logging, backup, troubleshooting	Availability, traceability, recoverability

3 Type of personal data

Group	Comprises
Master data	First name, surname, date and place of birth, nationality, address, position
Contact data	E-mail address, telephone number
Identity document data	Type, number, issuing authority and validity of the identity document; image of the document; result of the identity verification
Biometric data	Facial image from the identity document and from the live recording, and their automated comparison
Identification numbers	VAT identification number, register numbers; tax identification number only insofar as the Client is permitted to process it under § 139b(2) AO (Fiscal Code)
Ownership and structural data	Shareholder status, size of shareholding, status as beneficial owner, representation arrangements
Screening results	Hits and non-hits against sanctions and watch lists, PEP status, adverse media with sources

Group	Comprises
Client matter and contract data	Subject matter of the client relationship, insofar as required for risk classification; uploaded documents and their contents
Asset and financial data	Bank details, income and debt information, ownership of real estate and vehicles, land register data, social security number – only insofar as the questionnaire used by the Client collects them
Processing logs	User, time and type of entries, changes and confirmations relating to Client Matter Data
Access data of respondents	E-mail address, technical access key with expiry time, one-time code, access times, IP address

Special categories (Art. 9 GDPR). Biometric data is processed during identity verification insofar as the Client uses this procedure. Health data may be contained in uploaded medical documents; these are stored but their content is not analysed. Further special categories may be contained in adverse media screening hits; they are not analysed separately.

Data relating to criminal convictions and offences (Art. 10 GDPR) may be contained in hits from adverse media screening and in uploaded official documents, such as certificates of good conduct. A hit on a sanctions list does not in itself constitute information about a criminal offence. Processing takes place on the Client's instructions in order to fulfil its obligations under the GwG.

4 Categories of data subjects

Category	Description
Prospective clients	natural persons with whom the Client is assessing a client relationship
Clients	natural persons identified by the Client
Respondents	persons who enter information for a prospective client or client via a time-limited link, even if they are themselves neither a contracting party nor a beneficial owner
Legal representatives and authorised agents	managing directors, board members, authorised signatories (Prokuristen) and authorised agents of the clients
Beneficial owners	natural persons behind legal persons and legal arrangements
Shareholders and other participants	insofar as they appear in the ownership structure
Employees of the Client	as users processing Client Matter Data
Third parties from documents	persons named in uploaded documents

5 Locations of processing

The data is stored and processed within the European Economic Area: the application and file storage on Microsoft Azure in the Germany West Central region (Frankfurt am Main), the database with MongoDB Atlas in the same region, and the language model in the EU Data Zone. Annex 2 lists the sub-processors with their registered office, purpose and location of processing; clause 6.2 of the DPA applies to access from third countries.