Data Processing Agreement (DPA)

Version 1.3 | As of: 1 September 2026

The Data Processing Agreement is the legally binding version and is provided in German only. Please refer to the German version available on the Processor's website. For questions, contact legal@madita.ai. The following is a non-binding English summary of the agreement concluded between HeyJobs GmbH (processor) and our customers (controllers) under Art. 28 GDPR; in case of any discrepancy, the German version prevails.

Data Processing Agreement under Art. 28(3) GDPR

Between HeyJobs GmbH, Paul-Lincke-Ufer 39–40, 10999 Berlin, Germany, registered in the commercial register of the local court of Berlin-Charlottenburg under HRB 175212 B, VAT ID DE305584183, represented by the managing directors Marius Luther and Marius Jeuck (hereinafter “Processor”), and the natural or legal person that has registered via the Provider's platform and accepted this DPA electronically during registration or through order form (hereinafter “Controller” or “Customer”).

The master data provided during registration or through order form (in particular company name, address, registry court and number, authorised representative, business email address) becomes part of this DPA and identifies the Controller in a binding manner.

“Products” means, collectively or individually as the context requires, MADITA (standalone) and HeyMADITA, each as further defined as follows: “MADITA” means the AI-powered voice interview functionality described in this document when provided on a standalone basis, independent of any HeyJobs recruiting platform contract; “HeyMADITA” means the AI-powered voice interview functionality described in this document when activated as an add-on within a customer's existing HeyJobs recruiting platform contract under an active HeyJobs contract or agreement (FULLFLEX, HeyPakete, or REACH). Except where a provision expressly states that it applies only to HeyMADITA or only to MADITA, all provisions of this document apply equally to both Products.

Preamble

The parties have concluded a main contract (Order Form, General Terms and Conditions, hereinafter the “Main Contract”) on the provision and use of the Products. In the course of providing the service, the Processor

processes personal data on behalf of and according to the instructions of the Controller. This DPA specifies the parties' data protection rights and obligations under Art. 28 GDPR.

§ 1 Subject Matter, Duration and Termination

The subject matter of the DPA is the processing of personal data by the Processor on behalf of the Controller in the context of providing the Products, including all related functions (AI-powered voice interviews, transcription, competency-based preparation, reporting, ATS integration (if applicable), candidate communication). Where the Product is MADITA (standalone), the subject matter additionally includes ATS integration. Where the Product is HeyMADITA, no separate ATS integration is provided; HeyMADITA operates via the Controller's existing HeyJobs recruiting platform, and any data flows to or from an ATS occur exclusively within that HeyJobs platform relationship, outside the scope of this DPA.

This DPA begins with the entry into force of the main contract and ends automatically upon its termination; obligations that by their nature are intended to survive (in particular confidentiality, cooperation, deletion and return obligations) continue to apply. The Controller may extraordinarily terminate this DPA in the event of a serious breach by the Processor of data protection law or of material obligations under this DPA following an unsuccessful warning; such termination leads to the termination of the underlying main-contract relationship in accordance with the provisions of the main contract.

§ 2 Nature and Purpose of Processing

The Processor processes personal data exclusively to provide and operate the Products, to conduct AI-powered voice interviews, to create transcripts, competency assessments, summaries and highlights, to send invitations and reminders to candidates (where configured), to provide support and maintenance, and to anonymise data in accordance with § 17. For MADITA (standalone) only, the Processor additionally processes data to integrate with the Controller's ATS.

No further processing takes place without a documented instruction or a legal obligation. Processing is at all times and exclusively supportive; no autonomous or solely automated decision within the meaning of Art. 22 GDPR takes place (human-in-the-loop principle).

§ 3 Type of Personal Data

The following categories are processed in particular: identification and contact data of candidates (first and last name, email, telephone number, address where applicable), application documents (CV, cover letter, references where applicable), voice recordings from interviews (audio), interview transcripts, structured competency assessments, summaries and highlights, job postings and competency criteria, metadata (timestamps, language, session data, technical logs), and contact and login data of the Controller's recruiters.

Processing of special categories of personal data under Art. 9 GDPR is not envisaged. Should candidates volunteer such data, it is not used for assessment and is treated in accordance with the principles of data minimisation.

§ 4 Categories of Data Subjects

Applicants and candidates of the Controller, as well as recruiters and other employees of the Controller with access to the Products.

§ 5 Obligations and Rights of the Controller

The Controller remains responsible for the lawfulness of the data processing and for safeguarding the rights of the data subjects, and determines the purposes and means of processing alone.

The Controller is obliged in particular to determine and document the legal basis, to provide a suitable privacy notice to candidates (Art. 13/14 GDPR), to primarily fulfil data subject rights (Art. 15–22 GDPR) itself, to carry out a data protection impact assessment where required (Art. 35 GDPR), and to configure the assessment criteria in a non-discriminatory manner in accordance with the AGG. It designates a contact for the processing and, where required, a data protection officer.

§ 6 Obligations of the Processor

The Processor undertakes to process personal data exclusively on the basis of documented instructions (Art. 28(3)(a) GDPR), to ensure confidentiality (§ 8) and the security of processing (Art. 32 GDPR, § 9), to engage sub-processors only in accordance with § 10, and to support the Controller in fulfilling its obligations under Art. 32–36 GDPR and with data subject rights (Art. 12–22 GDPR).

It further undertakes to delete or return all personal data after completion of the processing at the Controller's choice (§ 15), to make available all information required to demonstrate compliance, and to enable audits in accordance with § 16. Data Protection Officer of the Processor, reachable at legal@madita.ai.

§ 7 Controller's Right to Issue Instructions

The Processor processes personal data only within the scope of the agreements and on the Controller's documented instructions; this DPA and the main contract constitute the initial documented instructions. Oral instructions must be confirmed without delay in text form (email suffices) to legal@madita.ai.

If the Processor considers that an instruction infringes applicable data protection law, it informs the Controller without delay and is entitled to suspend execution until the instruction is confirmed or amended. If a supervisory or law enforcement authority requests information or disclosure of data, the Processor informs the Controller without delay, to the extent legally permitted.

§ 8 Confidentiality

The Processor ensures that all persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory confidentiality obligation (Art. 28(3)(b), Art. 29, Art. 32(4) GDPR). The

confidentiality obligation continues beyond the end of the respective person's activity and beyond the end of this DPA. The Processor regularly trains its staff on data protection and data security.

§ 9 Technical and Organisational Measures (TOMs)

The Processor takes all technical and organisational measures required under Art. 32 GDPR to ensure a level of protection appropriate to the risk, in particular pseudonymisation and encryption of personal data, ensuring confidentiality, integrity, availability and resilience of systems, procedures for the rapid restoration of availability after incidents, and procedures for regularly reviewing the effectiveness of the measures.

The Processor is entitled to adjust the TOMs during the term, provided the level of protection is not thereby reduced; material changes are communicated in good time. The currently applicable version of the TOMs can be made available on request.

§ 10 Sub-processing

The Processor may engage sub-processors to fulfil its obligations. By concluding this DPA, the Controller grants general authorisation for the use of the sub-processors engaged by the Processor. The Processor informs the Controller at least 30 days before engaging a new or changing an existing sub-processor in text form; the Controller may object within 14 days for an important data protection reason. Absent an objection, the sub-processor is deemed approved.

In the event of a justified objection, the parties seek an amicable solution; if none is reached, the Controller may terminate the main contract with reasonable notice unless an equivalent replacement is named. The Processor binds each sub-processor by written contract to data protection obligations substantially equivalent to those in this DPA (Art. 28(4) GDPR). The current list of sub-processors can be made available on request. The sub-processor engaged for ATS integration (Kombo Technologies GmbH, or its successor) is engaged for MADITA (standalone) only and does not process data in connection with HeyMADITA.

§ 11 Transfers to Third Countries

Insofar as sub-processors are based in third countries outside the EEA, the transfer takes place on the basis of appropriate safeguards in accordance with Art. 44 et seq. GDPR. Insofar as recipients are based in the USA, the

transfer takes place in principle on the basis of an adequacy decision pursuant to Art. 45 GDPR, in particular on the basis of a certification under the EU-U.S. Data Privacy Framework (DPF), where such a certification exists. Where there is no certification under the DPF or no applicable adequacy decision, transfers take place on the basis of appropriate safeguards pursuant to Art. 46 GDPR, in particular the European Commission's Standard Contractual Clauses, supplemented where necessary by required additional safeguards.

§ 12 Assistance with Data Subject Rights

The Processor supports the Controller with appropriate technical and organisational measures in fulfilling data subject requests under Art. 12–22 GDPR. If a data subject contacts the Processor directly, it forwards the request to the Controller without delay and does not respond substantively.

The assistance includes in particular providing the data stored about a data subject in a structured, commonly used format, the technical implementation of rectification, erasure or restriction instructions, and providing required information. Effort for assistance beyond the standard scope may be provided against reasonable remuneration.

§ 13 Assistance with the Controller's Further Obligations

Taking into account the nature of the processing and the information available to it, the Processor assists the Controller in fulfilling the obligations under Art. 32–36 GDPR, in particular security of processing (Art. 32), notification of personal data breaches to the supervisory authority (Art. 33), communication to data subjects (Art. 34), data protection impact assessment (Art. 35) and prior consultation of the supervisory authority (Art. 36). It provides in particular a DPIA support package and a deployer guidance document on the EU AI Act.

§ 14 Personal Data Breaches

The Processor informs the Controller without delay after becoming aware of a personal data breach affecting data processed on the Controller's behalf. The notification contains at least a description of the nature of the breach, the approximate number of data subjects and records affected, the name and contact details of the point of contact, a description of the likely consequences, and of the remedial measures taken or proposed.

Where not all information is available at the same time, the notification is provided in stages without delay as it becomes available, to the point of contact named in § 7(2). The Processor promptly takes appropriate measures to secure the data and mitigate possible adverse consequences.

§ 15 Return and Deletion

After termination of this DPA, the Processor deletes or returns all personal data at the Controller's choice, unless a statutory retention obligation exists (Art. 28(3)(g) GDPR). The choice must be communicated in text form no later than 30 days after termination of the main contract; otherwise the Processor is entitled to delete the data after this period. Deletion takes place within 30 days of notification of the choice; the maximum period until complete deletion is 90 days from termination.

The default retention period for audio recordings and applicant-related processing results is 6 months after the completion of the respective application process (in accordance with Section 15 of the AGG); different retention periods can be set via the platform configuration. The Processor documents the deletion and provides a confirmation of deletion upon request. Anonymized data pursuant to Section 17 is not subject to this Section 15.

§ 16 Evidence and Audit Rights

The Processor makes available to the Controller on request all information required to demonstrate compliance with this DPA (Art. 28(3)(h) GDPR), in particular by presenting current certifications or audit reports of independent third parties. Where such evidence is insufficient, the Processor enables inspections by the Controller or an auditor commissioned by it (bound to confidentiality and not a competitor) after prior written notice with reasonable lead time during usual business hours.

§ 17 Anonymisation

The Controller is entitled and, at its own initiative, obliged to feed interview data collected in the context of the Services, prior to its final deletion, into an anonymisation pipeline that irreversibly removes personal identifiers so that re-identification is no longer possible (anonymisation within the meaning of Recital 26 GDPR).

Until anonymisation is completed, the Processor processes the data as a processor within the meaning of this DPA. After successful anonymisation, the data is no longer personal data; the provisions of this DPA do not apply to it. Further use of anonymised data is governed by the main contract.

§ 18 Liability

The liability of the parties is governed by the provisions of the main contract, unless mandatory statutory provisions, in particular Art. 82 GDPR, provide otherwise. Externally, vis-à-vis data subjects, Controller and Processor are liable under Art. 82 GDPR; internally, the apportionment is made according to the respective contributions to the cause. Any limitation of liability agreed in the main contract applies accordingly to liability under this DPA, to the extent legally permitted.

§ 19 Confidentiality of the DPA

The confidentiality of this DPA is governed by the main contract.

§ 20 Final Provisions

In the event of conflicts between this DPA and the main contract, the provisions of this DPA prevail with regard to data protection obligations. Amendments and supplements require text form (including the cancellation of this text-form requirement). Should any provision be or become invalid, the validity of the remaining provisions remains unaffected.

German law applies, excluding the UN Convention on Contracts for the International Sale of Goods and conflict-of-laws references, unless mandatory statutory provisions, in particular the GDPR, conflict. The exclusive place of jurisdiction is Berlin, to the extent legally permitted. A complete and up-to-date list of sub-processors and a current overview of the TOMs can be made available on request.

§ 21 Conclusion of Contract by Electronic Acceptance or Order Form

This DPA is concluded by the Controller accepting it electronically during registration by activating the relevant selection field and confirming (“click”). With this confirmation, the Controller simultaneously declares its agreement to the main contract (GTC) and the privacy policy. Electronic acceptance satisfies the text-form requirement under Art. 28(9) GDPR in conjunction with § 126b BGB; a handwritten signature is not required.

Where the Product is HeyMADITA, this DPA is concluded upon execution of the applicable Order Form referencing this DPA, rather than by electronic acceptance during platform registration. The Order Form's execution date and the Controller's identification data as stated in the Order Form constitute the record of conclusion for the purposes of this Section.

The Processor documents the conclusion of the contract by storing a timestamp, the accepted DPA version, the Controller's identification data and technical metadata (IP address, user agent). The applicable version is available and downloadable at any time on the Provider's website. For questions about the DPA or if you require a handwritten signed version, contact legal@madita.ai. Version history: v1.0 (19 May 2026) - initial publication; v1.1 (17 June 2026) - document URL update (legal-page localization); v1.2 (19 June 2026) - alignment with the applicable DPA version: Processor's Data Protection Officer (§ 6), third-country transfers (§ 11), extraordinary termination (§ 1), and provision of the TOMs and sub-processor list on request (§ 9, § 10, § 20); v1.3 (1 September 2026) - introduction of the Products/HeyMADITA/MADITA distinction (Preamble, parties clause), reliance on 'Processor' as the sole entity term throughout, Order Form-based conclusion for HeyMADITA (§ 21), and ATS integration/sub-processor scoping (§ 1, § 2, § 6, § 10).