Data Processing Agreement

between

_____

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

and

replient.ai Software GmbH, Derflerstraße 27/1, Lichtenberg, Austria

as the Processor (hereinafter the "**Processor**",
the Controller and the Processor together the "**Parties**")

Preamble

The Controller has engaged the Processor under the agreement already concluded (hereinafter the "**Main Agreement**") for the services specified therein. Part of the performance of the agreement is the processing of personal data. In particular, Art. 28 GDPR sets out certain requirements for such processing on behalf of a controller. To meet these requirements, the Parties conclude the following data

processing agreement (hereinafter the "**Agreement**"), the performance of which is not remunerated separately unless expressly agreed otherwise.

§ 1 Definitions

(1) Controller, pursuant to Art. 4(7) GDPR, is the body which alone or jointly with other controllers determines the purposes and means of the processing of personal data.

(2) Processor, pursuant to Art. 4(8) GDPR, is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

(3) Personal data, pursuant to Art. 4(1) GDPR, is any information relating to an identified or identifiable natural person (hereinafter the "**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) Special categories of personal data are personal data pursuant to Art. 9 GDPR revealing racial and ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of Data Subjects, personal data pursuant to Art. 10 GDPR relating to criminal convictions and offences 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 concerning the sex life or sexual orientation of a natural person.

(5) Processing, pursuant to Art. 4(2) GDPR, is any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(6) Supervisory authority, pursuant to Art. 4(21) GDPR, is an independent public authority established by a Member State pursuant to Art. 51 GDPR.

§ 2 Subject Matter of the Agreement

(1) The Processor provides the services specified in the Main Agreement for the Controller. In doing so, the Processor obtains access to personal data which it processes for the Controller exclusively on behalf of and in accordance with the instructions of the Controller. The scope and purpose of the data processing by the Processor result from the Main Agreement and any associated service descriptions. The assessment of the lawfulness of the data processing is incumbent on the Controller.

(2) To specify the mutual data protection rights and obligations, the Parties conclude this Agreement. In case of doubt, the provisions of this Agreement take precedence over the provisions of the Main Agreement.

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

(4) The term of this Agreement follows the term of the Main Agreement, unless the following provisions give rise to obligations or termination rights extending beyond it.

§ 3 Right to Issue Instructions

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

(2) The Controller's instructions are initially established by this Agreement and may thereafter be amended, supplemented or replaced by the Controller in writing or in text form by means of individual instructions (individual instruction). The Controller is entitled to issue corresponding instructions at any time. This includes instructions regarding the rectification, erasure and blocking of data.

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

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

§ 4 Types of Data Processed, Categories of Data Subjects, Third Country

(1) In the course of performing the Main Agreement, the Processor obtains access to the personal data specified in more detail in **Annex 1**.

(2) The categories of persons affected by the data processing are described in **Annex 2**.

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

§ 5 Protective Measures of the Processor

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

(2) Within its area of responsibility, the Processor shall organise its internal operations so as to meet the specific requirements of data protection. It has implemented the technical and organisational measures set out in **Annex 3** for the appropriate protection of the Controller's data pursuant to Art. 32 GDPR, which the Controller recognises as appropriate. The Processor reserves the right to modify the security measures taken, while ensuring that the contractually agreed level of protection is not undercut.

(3) Persons employed in data processing by the Processor are prohibited from collecting, processing or using personal data without authorisation. The Processor

shall obligate all persons entrusted by it with the handling and performance of this Agreement (hereinafter "**Employees**") accordingly (obligation of confidentiality, Art. 28(3)(b) GDPR) and shall ensure compliance with this obligation with due care.

(4) The Processor has appointed a data protection officer. The data protection officer of the Processor is heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Information Obligations of the Processor

(1) In the event of disruptions, suspicion of data protection breaches or breaches of the Processor's contractual obligations, suspicion of security-relevant incidents or other irregularities in the processing of personal data by the Processor, by persons employed by it within the scope of the engagement or by third parties, the Processor shall inform the Controller without undue delay. The same applies to inspections of the Processor by the data protection supervisory authority. 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, where possible including the categories and number of Data Subjects concerned and the categories and number of personal data records concerned;

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

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

(2) The Processor shall, without undue delay, take the necessary measures to secure the data and to mitigate possible adverse consequences for the Data Subjects, inform the Controller thereof and request further instructions.

(3) The Processor is further obliged to provide the Controller with information at any time, insofar as the Controller's data is affected by a breach pursuant to paragraph 1.

(4) The Processor shall inform the Controller of any material change to the security measures pursuant to § 5(2).

§ 7 Controller's Audit Rights

(1) The Controller may satisfy itself of the Processor's technical and organisational measures prior to the commencement of data processing and thereafter annually. For this purpose it may, for example, obtain information from the Processor, have existing expert reports, certifications or internal audits presented, or inspect the Processor's technical and organisational measures itself in person after timely coordination during normal business hours, or have them inspected by a qualified third party, provided that the latter is not in a competitive relationship with the Processor. The Controller shall carry out audits only to the extent necessary and shall not disproportionately disrupt the Processor's business operations.

(2) The Processor undertakes to provide the Controller, upon its oral or written request and within a reasonable period, with all information and evidence required to carry out an audit of the technical and organisational measures of the Processor.

(3) The Controller documents the result of the audit and communicates it to the Processor. In the event of errors or irregularities which the Controller identifies in particular when reviewing processing results, it shall inform the Processor without undue delay. If, during the audit, circumstances are identified whose future avoidance requires changes to the prescribed procedure, the Controller shall inform the Processor of the necessary procedural changes without undue delay.

§ 8 Engagement of Service Providers

(1) The contractually agreed services are performed with the involvement of the service providers named in **Annex 4** (hereinafter "**Sub-processors**"). The Controller grants the Processor its general authorisation within the meaning of Art. 28(2) sentence 1 GDPR to engage further Sub-processors or to replace those already engaged within the framework of its contractual obligations.

(2) The Processor shall inform the Controller in advance, by email newsletter, of any intended change regarding the engagement or replacement of a Sub-processor. The Controller receives the email newsletter after sending an email with the subject "Subscribe" to office@replient.ai. The Controller may object to an intended engagement or replacement of a Sub-processor on important data protection grounds.

(3) The objection to the intended engagement or replacement of a Sub-processor must be raised within 2 weeks of the dispatch of the information in the email newsletter. If no objection is raised, the engagement or replacement is deemed approved. If an important data protection ground exists and an amicable solution between the Controller and the Processor is not possible, the Controller is entitled to a special right of termination effective at the end of the month following the objection.

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

(5) A sub-processing relationship within the meaning of these provisions does not exist where the Processor commissions third parties with services that are to be regarded as mere ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific reference to services that the Processor provides for the Controller, and security services. Maintenance and inspection services constitute sub-processing relationships requiring consent insofar as they are provided for IT systems that are also used in connection with the provision of services for the Controller.

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

§ 9 Requests and Rights of Data Subjects

(1) The Processor supports the Controller, as far as possible, with appropriate technical and organisational measures in fulfilling its obligations under Art. 12–22 and 32 to 36 GDPR.

(2) If a Data Subject asserts rights, such as to information, rectification or erasure regarding its data, directly against the Processor, the Processor shall not act independently but shall refer the Data Subject to the Controller and await the Controller's instructions.

§ 10 Liability

(1) For the compensation of damage suffered by a Data Subject due to data processing or use that is unlawful or incorrect under the data protection laws within the scope of the processing on behalf of the Controller, the Controller alone is responsible vis-à-vis the Data Subject in the internal relationship with the Processor.

(2) The Processor is liable for damage without limitation insofar as the cause of the damage is based on an intentional or grossly negligent breach of duty by the Processor, its legal representative or vicarious agent.

(3) For negligent conduct, the Processor is liable only in the event of a breach of a duty whose fulfilment makes the proper performance of the Agreement possible in the first place and on whose observance the Controller regularly relies and may rely, but limited to the foreseeable damage typical of the contract. In all other respects, the liability of the Processor - including for its vicarious agents and assistants - is excluded.

(4) The limitation of liability pursuant to § 10.3 does not apply to claims for damages arising from injury to life, body or health or from the assumption of a guarantee.

§ 11 Termination of the Main Agreement

(1) Upon termination of the Main Agreement, the Processor shall return to the Controller all documents, data and data carriers provided to it or – at the Controller's request, unless an obligation to store the personal data exists under Union law or other applicable national law – delete them. This also applies to any data backups held by the Processor. The Processor shall, upon request, provide documented evidence of proper deletion.

(2) The Controller has the right to verify, in an appropriate manner, the complete and contractually compliant return or deletion of the data at the Processor.

(3) The Processor is obliged to treat the data that has become known to it in connection with the Main Agreement confidentially even beyond the end of the Main Agreement. This Agreement remains valid beyond the end of the Main Agreement for as long as the Processor holds personal data that was transmitted to it by the Controller or that it collected for the Controller.

§ 12 Final Provisions

(1) Insofar as the Processor does not expressly carry out support activities under this Agreement free of charge, it may charge the Controller a reasonable fee for them, unless the Processor's own acts or omissions made such support directly necessary.

(2) Amendments and supplements to this Agreement require text form. This also applies to the waiver of this formal requirement. The precedence of individual contractual arrangements remains unaffected.

(3) Should individual provisions of this Agreement be or become wholly or partially invalid or unenforceable, the validity of the remaining provisions shall not be affected thereby.

(4) This Agreement is governed by German law.

Controller

Name: _____

Position: _____

Date: _____

Signature: _____

Processor

Name: _____

Position: _____

Date: _____

Signature: _____

Annexes

Annex 1 – Description of the Data/Data Categories

In the course of providing the contractually agreed service (provision of a SaaS solution for AI-supported management, analysis and response to social media interactions as well as email drafting), the Processor obtains access to the following types and categories of personal data:

1. Master data / identification data:

- First and last names (e.g. of social media users, commenters, reviewers and senders)
- Profile names and usernames on the connected social media platforms (Meta, TikTok, LinkedIn, YouTube, Google)
- Email addresses

2. Content data:

- Texts of public social media comments and online reviews
- Contents of private direct messages (DMs).

Note: These are unstructured free-text fields that may potentially contain sensitive data voluntarily submitted by end users (e.g. private postal addresses, telephone numbers, order data or similar personal information).

- Contents of email conversations (when using the drafting function via Google Workspace / Outlook)
- "Learning" documents uploaded by the Controller (customer-specific information and training material for the AI)

3. Meta and communication data:

- IP addresses
- Social media profile IDs and user IDs
- Access tokens and authentication data (for connecting the API interfaces)
- Session data, HTTP request metadata and job reference IDs (during technical background processing)

4. Usage data:

- Log data and data on interaction with the software solution (usage behaviour)

Annex 2 – Description of the Data Subjects/Categories of Data Subjects

- **Users / employees of the Controller:** Employees and authorised persons of the Controller who use an account for the SaaS solution of replient.ai in order to manage comments and messages.
- **End customers and prospects of the Controller:** Persons who are in a business or pre-contractual relationship with the Controller and communicate with it via the connected channels.
- **Social media users and commenters:** Third parties who leave public comments on the Controller's profiles on the connected social media platforms (e.g. Meta, TikTok, LinkedIn, YouTube).
- **Authors of reviews:** Third parties who provide public reviews or ratings about the Controller on connected platforms (e.g. Google Reviews).
- **Senders of direct messages (DMs) and emails:** Persons who send the Controller private direct messages via the connected social media channels or emails, which are loaded into the replient.ai tool via the API interfaces and processed there.

Annex 3 – Technical and Organisational Measures of the Processor

Introduction

Controller

The controller pursuant to Art. 4 No. 7 of the EU General Data Protection Regulation (GDPR) is replient.ai Software GmbH, Derflerstraße 27/1, Lichtenberg, Austria, email: office@replient.ai. We are legally represented by Thomas Danninger, Markus Danninger.

Data Protection Officer

Our data protection officer is heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, email: datenschutz@heydata.eu.

Subject Matter of the Document

This document summarises the technical and organisational measures taken by the controller within the meaning of Art. 32(1) GDPR. These are measures by which the controller protects personal data. The purpose of the document is to support the controller in fulfilling its accountability obligation under Art. 5(2) GDPR.

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

Physical Access Control

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

- Chip card / transponder locking system
- Careful selection of cleaning staff
- Instruction to employees not to work in publicly accessible premises (e.g. cafés)
- Working from home: instruction to employees to work, where possible, in a study separated from living areas

System Access Control

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

- Authentication with username and password
- Automatic desktop lock
- General instruction to lock the desktop manually when leaving the workplace

Data Access Control

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

- Logging of access to applications (in particular for the entry, modification and deletion of data)
- The number of administrators is kept as small as possible
- Management of user rights by system administrators
- Instruction to employees that only strictly necessary data is printed
- Instruction to employees that data is deleted only after consultation

Separation Control

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

- Separation of production and test systems
- Definition of database rights

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

Transfer Control

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

- WLAN encryption (WPA2 with a strong password)
- Logging of access and retrievals

Input Control

The following measures ensure that it can be verified who processed personal data in data processing facilities and at what time:

- Logging of the entry, modification and deletion of data
- Creation of an overview of which applications can be used to enter, modify and delete which data
- Traceability of the entry, modification and deletion of data through individual usernames (not user groups)
- Instruction to employees to delete data only after consultation

Availability and Resilience (Art. 32(1)(b) GDPR)

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

- Regular backups

- Separation of operating systems and data
- Hosting (at least of the most important data) with a professional hosting provider

Procedures for Regular Review, Assessment and Evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

Data Protection Management

The following measures are intended to ensure that an organisation meeting the basic data protection requirements is in place:

- Use of the heyData platform for data protection management
- Appointment of heyData as data protection officer
- Obligation of employees to maintain data secrecy
- Regular data protection training for employees
- Maintaining a record of processing activities (Art. 30 GDPR)

Incident Response Management

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

- Reporting process for personal data breaches pursuant to Art. 4(12) GDPR to the supervisory authorities (Art. 33 GDPR)

- Reporting process for personal data breaches pursuant to Art. 4(12) GDPR to the Data Subjects (Art. 34 GDPR)

- Involvement of the data protection officer in security incidents and data breaches

Data Protection by Default (Art. 25(2) GDPR)

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

- Training of employees in "privacy by design" and "privacy by default"

- No more personal data is collected than is necessary for the respective purpose.

Commissioned Processing 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. by means of a data processing agreement)

- Ensuring the destruction of data after termination of the engagement, e.g. by requesting corresponding confirmations

- Confirmation from contractors that they obligate their own employees to maintain data secrecy (typically in the data processing agreement)

- Careful selection of contractors (in particular with regard to data security)

- Ongoing review of contractors and their activities

Annex 4 – Current Sub-processors

Name	Function	Server Location
Hetzner Online GmbH	Cloud hosting / data storage	EU (Germany)
Supabase, Inc.	Database-as-a-Service / backend / cloud storage	EU
Cloudflare, Inc.	CDN / DNS / DDoS protection / web application security	USA; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR); DPF certification in place.
OpenAI Ireland Ltd.	AI model/API / LLM functionality	USA / EU; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR).
Anthropic PBC	AI model/API / LLM functionality	USA; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR).
Google Ireland Limited	Cloud infrastructure / AI / Gemini / API interfaces	USA / EU (Ireland); SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR); DPF certification in place.
Inngest Inc.	Control of background processes (background jobs)	USA; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR).
Redis, Inc.	Database-as-a-Service	USA / EU; SCCs concluded

		(EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR).
Functional Software, Inc. (Sentry)	Application monitoring / error tracking	USA; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR); DPF certification in place.
Langfuse GmbH / Finto Technologies Inc.	AI monitoring / product analytics	EU / USA; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR).
Twilio Ireland Limited (SendGrid)	Email delivery (e.g. system notifications)	USA; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR); DPF certification in place.
Intercom R&D Unlimited Company	AI-supported customer support (live chat in the app)	USA; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR); DPF certification in place.
PostHog, Inc.	Product analytics	EU / USA; SCCs concluded (EU Standard Contractual Clauses pursuant to Art. 46(2)(c) GDPR); DPF certification in place.