DATA PROCESSING AGREEMENT (DPA)

Status: 12.02.2026

1. Scope

1.1. replient.ai Software GmbH, with its registered office in Lichtenberg, Austria, registered under FN671718x (hereinafter referred to as the "Processor"), shall provide all processing of personal data on behalf of its Controller (hereinafter each the "Controller" and each Controller together with the Processor the "Parties") based on this DPA, in each case in the version valid at the time of the contract conclusion.

1.2. The Processor may amend this DPA to reflect changes in legal requirements, technical developments, or the addition of new services. Any such amendments shall be communicated to the Controller at least thirty (30) days before they take effect. The Controller may object in writing to office@replient.ai within thirty (30) days of receiving such notice. If the Controller objects, the Controller may terminate its account and the associated Main Agreement before the effective date of the amendment, without penalty. If the Controller does not object or terminate the account within the thirty (30) day period, the amendment shall be deemed accepted and will become effective at the end of that period.

1.3. The Processor shall carry out the processing of personal data described in Annex 1 on behalf of the Controller under the Main Agreement concluded between the Parties for using the Replient.ai services (hereinafter the "Main Agreement").

2. Place of Processing

2.1. The Data Processing shall take place in a member state of the European Union or another contracting state of the Agreement on the European Economic Area unless otherwise agreed between the Parties. The Data Processing by the sub-processors named in Annex 1 shall be deemed approved at the locations named in Annex 1.

2.2. Any transfer of Data Processing to a third country requires the prior consent of the Controller and may only occur if the requirements of Art 44 et seq GDPR are met.

3. Obligations of the Processor

3.1. The Processor undertakes to carry out Data Processing exclusively based on documented instructions from the Controller. If the Processor considers an instruction of the Controller to be unlawful, the Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller.

3.2. The Processor shall treat confidentially any personal data it becomes aware of in connection with the Data Processing. The Processor shall impose a confidentiality obligation on all persons authorized by it to process the data, unless they are already subject to a statutory duty of confidentiality. The obligation of confidentiality and non-disclosure shall continue after termination of this DPA.

3.3. The Processor shall implement and maintain the technical and organisational measures described in **Annex 2 – Technical & Organisational Measures (TOM)**, which forms an integral part of this Agreement. The Processor shall regularly review and, where necessary, update these measures to ensure a level of security appropriate to the risk pursuant to Art. 32 GDPR. Material changes shall be notified to the Controller in writing at least 30 days in advance.

3.4. The Processor shall, where possible, support the Controller with appropriate technical and organizational measures to enable the Controller to comply with the data subject rights under Chapter III of the GDPR within the legal time limits and shall provide the Controller with the necessary information to do so upon the Controller's request, provided that the Processor has such information. If a subject submits a request to the Processor to exercise the data subject rights, the Processor shall be obliged to forward the request to the Controller if the request relates to Data Processing by the Controller.

3.5. The Processor shall support the Controller in performing the obligations incumbent upon the Controller pursuant to Art. 32 to 36 of the GDPR, including the implementation of security measures, the notification of data protection breaches, and, where applicable, the preparation of a data protection impact assessment. The Processor shall notify the Controller without undue delay, and in any event within 24 hours after becoming aware of a personal data breach. The notice shall at least contain the information set out in Art. 33 (3) GDPR. The Processor shall cooperate with the Controller and provide all reasonable assistance to enable the Controller to meet its obligations under Art. 33 and 34 GDPR

3.6. The Processor shall delete the personal data of the Data Processing after the expiry of the retention periods provided for in the Main Agreement and/or without delay at the request of the Controller. If the Controller expressly requests this, the personal data shall be returned to the Party. Statutory retention periods remain unaffected by this.

3.7. The Processor is obliged to provide the Controller with information at the latter's request to demonstrate compliance with the obligations pursuant to Art. 28 of the GDPR. The Processor shall support the Controller in verifying the Data Processing and shall grant the Controller access to the documents and technical systems necessary for verifying the Data Processing in accordance with Section 5 of this DPA.

3.8. To the extent permitted by law, the Processor shall inform the Controller about control actions and measures taken by the supervisory authorities insofar as they relate to the Controller's Data Processing operations.

4. Sub-Processor

4.1. The Controller expressly authorizes the use of the services of sub-processors by the Processor in performing the Data Processing operations. The sub-processors listed in Annex 1 shall be deemed approved at the time of contract conclusion.

4.2. The Processor shall inform the Controller of any intended change regarding the use or replacement of a sub-processor. The Controller may object to the intended change in writing by email to office@replient.ai within 30 working days from the date of notification. In case of timely objection, the Processor shall not be entitled to use the services of the rejected sub-processor in the Data Processing operations. If no objection is raised by the Controller within the aforementioned period, the intended change shall be deemed approved by the Controller.

4.3. If the Processor uses a sub-processor, it shall be obliged to conclude an agreement with the sub-processor within the meaning of Art. 28(4) of the GDPR. In this agreement, it must be ensured that the sub-processor enters into the same obligations that apply to the contractor based on this DPA.

5. Rights of Control and Inspection

The Controller shall have the right, upon reasonable prior notice, to verify the Processor’s compliance with this DPA and applicable data protection law. Such audits may be conducted by the Controller or by an independent auditor mandated by the Controller, during regular business hours and in a manner that minimizes disruption to the Processor’s operations. The Processor may demonstrate compliance through relevant documentation, security summaries, or third-party assessments, and, where available, certifications or external audit reports. Each Party shall bear its own costs of any audit; additional audits beyond one (1) per year shall be subject to prior agreement on reasonable compensation for the Processor’s internal efforts.

6. Remuneration

The Processor assists in complying with the Controller's obligations under data protection law to a reasonable extent without additional costs. If the requested assistance in complying with the Controller's data protection obligations exceeds the reasonable extent, the Processor shall inform the Controller accordingly and provide a cost estimate for these services. These services exceeding the reasonable extent of the appropriate scope will be provided by the Processor on the basis of the cost estimate after being commissioned by the Controller. The reasonable extent of the scope of the annual review and inspection is determined by the Processor.

7. Term

The term of this DPA corresponds to the term of the Main Agreement plus the retention period provided for therein.

8. Final Provisions

8.1. This DPA shall be governed by and construed in accordance with the laws of a Member State of the European Union. The Parties agree that Austrian law shall apply, excluding any rules of private international law that would result in the application of non-EU law.

8.2. Should individual provisions of this DPA be or become invalid, this shall not affect the remaining content of the DPA. The invalid provision shall be replaced by a valid provision that is legally valid and comes as close as possible to the economic intent of the Parties. The same shall apply in the event of a loophole in the contract.

Annex 1 - Description of Data Processing

1. **Subject of the Data Processing:**
   - Operation of a social media management tool that allows the client to manage comments on Facebook and Instagram, analyze sentiment, and automate replies.
2. **Duration of Data Processing:**
   - During the term of the Main Agreement and the retention periods provided for therein.
3. **Nature and Purpose of the Data Processing:**
   - Data from social media networks is imported into the tool operated by the Processor via interfaces provided by the networks. The purpose is to manage social media interactions, plan, and publish content, and centralize all social media communication.
4. **Categories of Personal Data:**
   - First and last name, user IDs, profile URLs, profile pictures, website URLs, timestamps, posting IDs, posted texts, pictures, videos, links, comments, ratings, private messages, other attachments, and metadata of social media content.
5. **Categories of Data Subjects:**
   - Users of the social media platforms used.
6. **Authorized Sub-Processors:**
   - Hosting and database: Supabase (AWS data centers in Frankfurt)
   - Hosting: Hetzner (EU data center in Frankfurt)
   - Email: Sendgrid (EU data centers)
   - Language Processing: OpenAI Ireland Ltd (Ireland): Data may, to a limited extent, be accessed by OpenAI OpCo, LLC (USA) as part of OpenAI's internal service architecture. Any such transfer is governed by the EU Standard Contractual Clauses (SCC Module 3 – Processor to Sub-Processor) between OpenAI Ireland Ltd. and OpenAI OpCo, LLC, supplemented by additional safeguards including encryption in transit, strict access control, and minimization of personal data. Processing by OpenAI Ireland Ltd. and its affiliates complies with the Data Processing Addendum in force between the Processor and OpenAI Ireland Ltd., which forms part of this DPA by reference.

The technical and organisational measures are outlined in Annex 2 of this Agreement

Annex 2 - Technical & Organisational Measures (TOM)

#	Area	Measure (Replient.ai – "Processor")
1	Confidentiality	• *Hosting:* Hetzner Cloud, data-centre **nbg1-dc3**, Nürnberg (ISO 27001, biometric & key-card access, 24/7 CCTV). • *Access control:* Role-based, least-privilege; admin accounts require MFA; server access via SSH keys; all employees under NDA. • *Pseudonymisation & segregation:* Where feasible, personal identifiers are replaced with tokens before processing; customer data separated via Supabase row-level security & auth scopes.
2	Integrity & Transmission	• All external traffic secured with **HTTPS / TLS 1.2+**. • Data at rest encrypted with **AES-256** on Hetzner volumes and Supabase managed Postgres/storage. • Audit & input control via immutable Supabase logs and application audit trails.
3	Availability & Resilience	• Supabase automated **daily backups**, 7-day retention; encrypted and stored in EU region. • Target: ≤ 24 h Recovery Time Objective (RTO) & ≤ 1 h Recovery Point Objective (RPO). • Hetzner UPS, redundant power & network; continuous monitoring & alerting.
4	Regular Testing & Evaluation	• Annual external penetration test & quarterly vulnerability scans. • Security awareness training for all staff; documented incident-response playbooks; change management with code review & CI pipeline.
5	Supplementary Measures for non-EU Sub-processors (OpenAI)	• Text prompts - including publicly available comment data (e.g., usernames and comment content from social media platforms) and, where applicable, private messages submitted via supported APIs - may be transmitted to OpenAI Ireland Ltd. for language processing. • Such prompts may include personal data as defined in Art. 4(1) GDPR, particularly in the case of private messages. Therefore, OpenAI Ireland Ltd. is listed as an authorized sub-processor in Annex 1. • The transfer is secured via TLS encryption and takes place under Standard Contractual Clauses (SCC) Module 3, supplemented with additional contractual safeguards (e.g. encryption in transit, prohibition of unlawful governmental access, and transparency commitments). • Data minimization principles are applied: only essential contextual input is transmitted for processing. Outputs are logged exclusively in the EU and retained for a maximum of 30 days for traceability and quality assurance.