ADDENDUM
DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") will take effect as of [*Insert date*] ("**Effective Date**")

BETWEEN

[*Insert name of entity*], a [●] established and existing under the laws of [●], having its registered office at ([●]) [●], [●], at the address [●], hereinafter referred to as: "**Controller**",

and

Custodea B.V. a private limited company established and existing under the laws of the Netherlands, having its registered office in Utrecht, at the address Schönberglaan 26, hereinafter referred to as: "**Processor**",

each a "**Party**" and collectively the "**Parties**".

RECITALS

(A) On [*Insert date*] Controller and Processor entered into an agreement (the "**Agreement**") pursuant to which Processor will provide certain services (the "**Services**") to Controller.

(B) To the extent that the provision of such Services involves the processing of personal data, the Parties have agreed to enter into this DPA for the purposes of ensuring compliance with the applicable Data Protection Laws, as defined below.

THEREFORE, the Parties have agreed as follows:

1. DEFINITIONS

1.1 Terms such as "processing", "data subject", "processor", "controller", "personal data", "data protection impact assessment", etc., shall have the same meaning ascribed to them in the Data Protection Laws;

1.2 "**Adequate Third Country**" means a country which is not a member of the EEA and where there is an existing decision by the European Commission pursuant to Article 45 GDPR that confirms that such country ensures an adequate level of protection for personal data;

1.3 "**Data Protection Laws**" means in relation to any Personal Data which is Processed in the performance of the Agreement, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") together with all laws implementing or supplementing the GDPR and any other applicable data protection or privacy laws, including any regulations, guidance, and codes of practice issued by Supervisory Authorities from time to time;

1.4 "**EEA**" means the European Economic Area;

1.5 "**Personal Data**" means the data described in Schedule 1 (*Details of Processing of Personal Data*) and any other personal data processed by Processor or any Subprocessor on behalf of the Controller pursuant to or in connection with the Agreement;

1.6 "**Personal Data Breach**" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised, disclosure or access to Personal Data;

1.7 "**Services**" means the services described in the Agreement;

1.8 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to third countries, adopted by the European Commission via its implementing decision of 4 June 2021, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;

1.9 "**Subprocessor**" means any processor (including any third party and any affiliated company) appointed by Processor to process personal data on behalf of Controller; and

1.10 "**Supervisory Authority**" means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws.

2. OBLIGATIONS OF CONTROLLER

2.1 Controller warrants that it will comply with its obligations and responsibilities under the Data Protection Laws including but not limited to ensuring that it has:

2.1.1 complied with transparency obligations including ensuring that an notice is made available to the relevant data subject(s) which adequately covers the processing activities of Processor;

2.1.2 determined a lawful basis for the processing of the Personal Data and obtained any necessary consents or permissions from data subjects; and

2.1.3 taken reasonable steps to ensure that the personal data is accurate.

3. PROCESSING OF THE PERSONAL DATA

3.1 Processor shall only process the types of Personal Data relating to the categories of data subjects as instructed by the Controller and for the specific purposes in each case as set out in Schedule 1 (*Details of Processing of Personal Data*) to this DPA and shall not process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party other than in accordance with Controller's documented instructions unless such processing is required by EU or Member State law to which Processor is subject, in which case Processor shall inform Controller of that legal requirement before processing that Personal Data unless the law prohibits this.

3.2 For the purposes set out in section 3.1 above, Controller hereby permits Processor to transfer Personal Data to the recipients listed in Schedule 2 (*Authorised Transfers of Controller Personal Data*) always provided that Processor shall comply with section 6 (*Subprocessing*) and 12 (*International Transfers of Personal Data*).

3.3 Processor shall immediately inform Controller if in Processor's opinion the instructions given by Controller infringe applicable Data Protection Laws.

3.4 The Processor may use data derived from the Personal Data for its own internal business purposes only where and to the extent such data has been anonymised in

accordance with applicable Data Protection Laws and no longer relates to an identified or identifiable natural person.

4. PROCESSOR PERSONNEL AND CONFIDENTIALITY

4.1 Without prejudice to any existing contractual arrangements between the Parties, Processor shall treat all Personal Data as strictly confidential and shall take reasonable steps to ensure the reliability of any volunteer, agent, employee, contractor and/or Subprocessor who may have access to the Personal Data.

4.2 Processor shall ensure that all such persons or parties involved in the processing of Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. SECURITY

5.1 Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks in accordance with article 32 GDPR. This includes protecting the Personal Data against a Personal Data Breach. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

6. SUBPROCESSING

6.1 Processor has Controller's general authorisation to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6.

6.2 Processor may continue to use those Subprocessors already engaged by Processor as at the Effective Date and included in Schedule 2 (*Authorised Subprocessors*) provided that in each case Processor meets the obligations set out in section 6.4.

6.3 Processor shall inform the Controller in advance of the appointment of any new Subprocessor and give the Controller the opportunity raise reasonable objections to such appointment. If the Controller does not notify the Processor of any objections in writing within 10 days of such notice, the Processor may appoint the Subprocessor. If the Controller notifies Processor of reasonable objections in writing within 10 days of such notice, the Parties will discuss possible resolutions.

6.4 With respect to each Subprocessor, Processor shall:

6.4.1 include terms in the contract between Processor and each Subprocessor which are in substance the same as those set out in this DPA, and shall supervise compliance thereof;

6.4.2 to the extent that the appointment of the Subprocessor involves a transfer outside of the EEA, comply with section 12.2; and

6.4.3 remain fully liable to Controller for any failure by each Subprocessor to fulfil its obligations in relation to the processing of any Personal Data.

7. DATA SUBJECT RIGHTS

7.1 Processor shall promptly notify Controller if it receives a request from a data subject under any Data Protection Laws in respect of Personal Data, including requests by a data subject to exercise rights in chapter III of GDPR, and shall provide full details of that request.

7.2 Processor shall co□operate and assist as requested by Controller to enable Controller to comply with its obligations to respond to any exercise of rights by a data subject under any Data Protection Laws in respect of Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Personal Data or this DPA. In each case Controller shall reimburse Processor for costs (including internal resources and necessary third-party costs) reasonably incurred by Processor where such assistance goes beyond the Services provided under the Agreement.

8. INCIDENT MANAGEMENT

8.1 In the event of a Personal Data Breach, Processor shall immediately take appropriate measures to address the Personal Data Breach including measures to mitigate its adverse effects.

8.2 Processor shall notify Controller without undue delay upon becoming aware of a Personal Data Breach and will provide Controller with sufficient information which allows Controller to meet its obligations to report a Personal Data Breach under the Data Protection Laws. Processor shall use commercially reasonable efforts to:

8.2.1 describe the nature of the Personal Data Breach, the categories and numbers of data subjects concerned, and the categories and numbers of Personal Data records concerned;

8.2.2 communicate the name and contact details of Processor's data protection officer or other relevant contact from whom more information may be obtained;

8.2.3 describe the likely consequences of the Personal Data Breach; and

8.2.4 describe the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects;

8.3 Processor shall co-operate with Controller and take such reasonable steps as are directed by Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach, in order to enable Controller to *(i)* perform a thorough investigation into the Personal Data Breach, *(ii)* formulate a correct response and to take suitable further steps in respect of the Personal Data Breach in order to meet any requirement under the Data Protection Laws. Controller shall reimburse Processor for costs reasonably incurred by Processor where such assistance goes beyond the Services provided under the Agreement.

9. ASSISTANCE TO THE CONTROLLER

9.1 Processor shall provide reasonable assistance to Controller with any data protection impact assessments or with any prior consultations to any Supervisory Authority of Controller which are required under Data Protection Laws, in each case in relation to processing of Personal Data by Processor on behalf of Controller and taking into account the nature of the processing and information available to Processor.

10. DELETION OR RETURN OF CONTROLLER PERSONAL DATA

10.1 Processor shall promptly, upon termination of the Services and at the choice of Controller either:

10.1.1 return a complete copy of all Personal Data to Controller by secure file transfer in such format as notified by Controller to Processor; or

10.1.2 securely wipe all copies of Personal Data processed by Processor,

unless applicable law requires such storage of Personal Data, in which case Processor will inform Controller of such obligation (including details of the Personal Data it is required to retain and a specific timeline for destruction once the legal requirement ends).

11. AUDIT RIGHTS

11.1 Processor shall make available to Controller on request all information necessary to demonstrate compliance with this DPA.

11.2 Controller's audit rights in relation to Processor's compliance with this DPA and Applicable Data Protection Law are exclusively set out in the Agreement. No additional audit, inspection or access rights shall apply unless expressly agreed in writing by the Parties.

12. INTERNATIONAL TRANSFERS OF CONTROLLER PERSONAL DATA

12.1 The Parties acknowledge and agree that the Processor will process the Personal Data within the EEA. The Processor will not process personal data outside of the EEA without first informing the Controller and executing adequate safeguards including Standard Contractual Clauses (*Module 2 – Controller to Processor*) where necessary.

12.2 To the extent Controller authorizes Processor to appoint a Subprocessor in accordance with section 6 and such Subprocessor processes Personal Data in a country outside the EEA, Processor shall prior to such appointment complete and execute *Module 3* Standard Contractual Clauses (*Transfer processor to processor*) with the Subprocessor.

12.3 If, at any time, the European Commission, a Supervisory Authority or a court with competent jurisdiction over a Party mandates that transfers from controllers in the EEA to processors established outside the EEA must be subject to specific additional safeguards, the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of Personal Data is conducted in compliance with such mandate.

12.4 If, and to the extent that, the European Commission issues any amendment to, or replacement of, the Standard Contractual Clauses pursuant to Article 46(5) GDPR, the Parties acknowledge and agree that such clauses will automatically be deemed to replace all Standard Contractual Clauses then in force between Controller on the one hand and Processor on the other and the Parties shall take such additional steps as necessary to ensure that such replacement terms are implemented across all transfers.

13. MISCELLANEOUS

13.1 The Parties agree that this DPA shall terminate automatically upon termination of the Agreement.

13.2 This DPAt shall be read and interpreted in the light of the provisions of the Data Protection Laws. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including but not limited to the Agreement, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations for Personal Data. In the event of any conflict or inconsistency between this DPA and any executed Standard Contractual Clauses between Controller and Processor, such Standard Contractual Clauses shall prevail.

13.3 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either *(i)* amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, *(ii)* construed in a manner as if the invalid or unenforceable part had never been contained therein.

13.4 This DPA is governed by the laws of the Netherlands. Any disputes arising out or in connection with this DPA shall be brought exclusively before the competent court of Amsterdam.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the Effective Date first set out above.

[Insert Entity Name Here]	**[Insert Entity Name Here]**
Signature	Signature
for and on behalf of [Entity Name]	for and on behalf of [Entity Name] (Processor)
Name	Name
Title	Title
Date	Date

SCHEDULE 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Schedule 1 includes certain details of the processing of Personal Data as required by Article 28(3) GDPR.

1. Subject matter, duration and purposes of the processing of Personal Data

1a. Subject matter of the processing:

Processing of Personal data as necessary to perform the Services described in the Agreement (including data collection, analysis, visualisation and impact measurement services).

1b. Duration of the processing:

The duration of the processing of Personal Data by Processor under this DPAis the period of the Agreement.

1c. *Frequency of the processing*:

The Personal Data will be shared on the following basis during the period of the Agreement.

□ one-off

□ continuous

□ Other (please specify)

1d. Nature and Purpose of the processing:

The purpose of the processing of Personal Data by Processor under this DPAt is the performance of the services as described in the Agreement.

2. The categories of data subject to whom the Personal Data relates

□ Employee data

□ Customer data

□ Other (please specify)

3. The types of Personal Data to be processed

<u>1. Employees</u>

□ **Employee data**, more in particular:

□ *Personal details* - such as name and first name, address, email address, telephone number or other contact information, degree/title, date of birth, gender, nationality, social security or national insurance number, marital or civil partnership status, domestic partners, dependents, citizenship.

- □ *Emergency contact details* - name and contact details of emergency contacts.
- □ *Financial details* - such as bank account details or other financial characteristics.
- □ *Basic work details* - such as work contact details e.g. corporate email address and telephone number, employee identification number, photograph, details regarding the job function, primary work location, working hours, employment status, and terms and conditions of employment, immigration status, work permit details.
- □ *System and application access data* - information required to access Controller's systems and applications such as email account and system passwords, or device information of e.g. mobile phones or laptops.
- □ *Electronic localisation data* - such as GPS position obtained from track & trace systems that are placed in company vehicles.
- □ *Professional qualifications* - professional certifications, special skills including (driver) licenses, language skills, memberships of committees or other bodies, education history.
- □ *Recruitment or selection data* - any personal data contained in CV's, application forms, references, record of interviews or interview notes, and selection and verification records, previous (job) experiences and references.
- □ *Video surveillance footage* - as recorded in buildings by the use of video surveillance equipment (CCTV).
- □ *Remuneration and benefits data* - such as details of payment and benefits package, base salary, bonus, compensation type, long term incentives, company credit card data, tax information, salary reviews.
- □ *Leave data* - such as holiday and family related leave records, retirement eligibility.
- □ *Performance management data* - such as colleague and manager feedback, appraisals, outputs from talent programs and formal and informal performance management processes.
- □ *Training and development data* - such as data relating to training and development needs or trainings received.
- □ *Documentation required under immigration laws* - such as citizenship, details of residency, work permit.
- □ *Psychological data* - for example, personality questionnaires as part of an assessment.
- □ *Disciplinary data* - such as any personal data contained in records of allegations, investigation and proceeding records and outcomes, and in the context of whistleblowing.
- □ *Termination data* - such as dates and reasons for leaving, termination agreements and payments, exit interviews and references.
- □ *Special categories of data (sensitive data)* - such as physical or mental health data (e.g. days and reasons of sickness, workplace amendments), racial or ethnic origin, religious or similar beliefs, membership of a trade union, the commission or alleged commission by the employee of any offence; and any proceedings for any offence committed or alleged to have been committed by the employee, the disposal of those proceedings or the sentence of any court in those proceedings, or any other judicial measures such as court seizures or individual traffic fines by using a company vehicle.
- □ *Other data* - please specify.

2. Customers

□ **Controller's customer data**, more in particular:

□ *Contact details* - such as name, postal address and other contact details, such as telephone number and e-mail address or any other contact details.

□ *Personal characteristics* - such as gender or other personal characteristics in order to identify representatives of customers.

□ *Profession and job title* - including information on the specific (sub) sector the customer operates in.

□ *Data collected automatically through websites* - such as cookies and other technologies to track website visitors.

□ *Financial details* - such as bank account details or invoicing details.

□ *Information relating to the use of services* - such as which services are used or contracted.

□ *Pictures* - to identify the customer (representative).

□ *Communication data* - such as any requests, any complaints and any other customer data that Controller receives when communicating with customers via email, online or via social media.

□ *Other data* - please specify.

SCHEDULE 2: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

#	Sub-processor	Location	Role	Categories of data
1	Hetzner Online GmbH	Germany (Falkenstein); backup region Finland (Helsinki)	Infrastructure hosting for the entire Custodea platform	All Customer Data at rest and in transit within the platform
2	Cloudfleet	Germany	Managed Kubernetes control plane (cluster-level administrative access)	Potentially all platform data (administrative access only)
3	Proton AG	Switzerland (EU adequacy decision)	Business e-mail	Correspondence and contact details, which may include Customer Personal Data
4	Lettermint B.V.	Netherlands	Transactional platform e-mail	User names and e-mail addresses
5	Mistral AI	France	Large-language-model inference for the optional chat feature	Chat prompts and query results, which may include Customer Personal Data
6	Scaleway	France	LLM hosting (chat feature)	Same as Mistral AI

ANNEX 3: DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE PERSONAL DATA

All measures below are implemented today unless explicitly marked otherwise.

1. Encryption and pseudonymisation

- Full-disk encryption (LUKS2) on all object-storage nodes (data, filer and metadata devices).
- Application-level AES-256-GCM encryption of connector credentials and OAuth tokens; encryption keys are stored outside the database.

- TLS for all data in transit (public endpoints and internal service traffic).
- Pseudonymisation of Dutch citizen service numbers (BSN) via per-tenant keyed HMAC for healthcare data sources; configurable exclusion of sensitive tables.

2. Tenant isolation

- Dedicated object-storage bucket per customer; no shared buckets.
- Dedicated lakehouse catalogue database per customer.
- Dedicated Kubernetes namespace per customer with namespace-scoped RBAC and secrets.
- Network segmentation via Kubernetes NetworkPolicies on every service.
- Scoped IAM credentials per tenant; per-user storage policies restricted to key prefixes.

3. Access control

- Single sign-on via self-hosted identity provider (Keycloak); role-based authorisation in the application.
- PostgreSQL row-level security (FORCE) with per-user grants compiled from customer-defined access policies.
- Administrative access exclusively via authenticated mesh VPN; no publicly exposed administrative interfaces.
- Multi-factor authentication: enforced for all administrative and staff access (identity provider level). Customer users authenticating via their organisation's identity provider (Microsoft / Google single sign-on) inherit that organisation's MFA policy; native multi-factor authentication for password-based customer accounts is planned (target Q4 2026).

4. Logging, monitoring and audit

- Append-only audit events for all organisation- and configuration-level changes, written transactionally.
- Per-request audit records on the data-access layer (tool-level logging for AI/API access).
- Build-time enforcement that chat/message content is never written to application logs.
- Central log retention: 30 days (stated plainly; the Annex makes no longer-retention promise).

5. Availability and backups

- Daily automated backups; primary region Germany, backup region Finland (both EU).
- Daily automated backups with a 30-day retention window; after erasure, tenant data disappears from all backups within 30 days (well within the 90-day commercial commitment).

6. Data minimisation

- Extraction-only architecture: raw source data is stored without enrichment or profiling.
- Configurable per-stream column redaction; sensitive-table exclusion lists per connector.

7. Deletion

- Documented tenant teardown procedure covering pipeline deployments, lakehouse catalogue, object-storage bucket and credentials.

8. Organisational measures

- Information-security programme structured along the NBA-LIO maturity model, target maturity level 3 on all controls.
- Secrets management via encrypted vaults (SOPS / sealed secrets); no credentials in source control or databases.
- All changes to production via reviewed pull requests and CI pipelines.
- Personal-data-breach handling: breaches are contained and notified to the Controller in accordance with the notification obligations and timelines set out in this DPA.