Data Processing Agreement

Agreement pursuant to Article 28(3) UK GDPR
Edith Care (Jobello Technology AB)

Based on the Edith Care personuppgiftsbiträdesavtal (SKR/Inera/Adda template v2.1), adapted for UK GDPR · Version 2026-07-12-uk-v1

CONTENTS

DATA PROCESSING AGREEMENT

Agreement pursuant to Article 28(3) UK GDPR

1. PARTIES, ROLES, CONTACT DETAILS AND CONTACT PERSONS

	Controller	**Processor**
Entity	The organisation on whose behalf this DPA is accepted at account registration (section 22), as identified by the registration details	Edith Care (Jobello Technology AB)
Registration no	As provided at account registration	Swedish company reg. no 559311-6907
ICO registration no	As provided at account registration, where registered	n/a for this Processing (registration attaches to controllers; the Processor's own controller-capacity registration, where applicable, is separate)
Address	As provided at account registration	Sveavägen 119, 113 49 Stockholm, Sweden
UK representative (Art 27 UK GDPR)	n/a (UK-established)	Appointment in progress; the Processor will notify the Controller of the representative's details in writing upon appointment
Responsible for this DPA and data protection cooperation	The registering user, unless the Controller notifies the Processor of another contact in writing	Fredrik Gordh Riseby, CEO, fredrik@edithcare.se

2. DEFINITIONS

Terms capitalised in this DPA have the meanings below, whether used in singular or plural:

- **Processing** — any operation or set of operations performed on Personal Data, whether or not by automated means (collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).
- **Data Protection Legislation** — all privacy and data protection law applicable to the Processing under this DPA, including the UK GDPR, the Data Protection Act 2018 and any legislation replacing or supplementing them.
- **Controller / Processor / Data Subject / Personal Data / Personal Data Breach** — as defined in the UK GDPR.
- **Instruction** — the written instructions specifying the subject matter, duration, nature and purpose of the Processing, the types of Personal Data, the categories of Data Subjects and any special requirements (Annex 1).
- **Log / Logging** — the continuous collection of records of the Processing that can be attributed to an individual natural person, and the resulting records.
- **Third Country** — a country other than the United Kingdom or a member state of the EU/EEA.
- **Sub-processor** — a natural or legal person engaged by the Processor to Process Personal Data on behalf of the Controller.

3. BACKGROUND AND PURPOSE

3.1 This Data Processing Agreement, together with its Instruction (Annex 1) and the list of approved Sub-processors (Annex 2) (jointly the "DPA"), governs the Processor's Processing of Personal Data on behalf of the Controller. Its purpose is to safeguard the rights and freedoms of Data Subjects in accordance with Article 28(3) UK GDPR.

3.2 Where this DPA forms part of a wider agreement, that agreement is referred to as the "Main Agreement". If anything in sections 1, 3.2, 15, 16, 17.6, 18–20 or 22 of this DPA is regulated differently in the Main Agreement, the Main Agreement prevails.

3.3 References to legislation are to that legislation as amended and in force from time to time.

4. PROCESSING OF PERSONAL DATA AND SPECIFICATION

4.1 The Controller hereby appoints the Processor to carry out the Processing on the Controller's behalf as set out in this DPA.

4.2 The Controller shall give written Instructions to the Processor on how the Processing is to be performed.

4.3 The Processor may only carry out the Processing in accordance with this DPA and the Instructions in force from time to time.

5. RESPONSIBILITIES OF THE CONTROLLER

5.1 The Controller is responsible for ensuring that a lawful basis exists for the Processing at all times — for health data, Article 9(2)(h) UK GDPR in combination with the condition in paragraph 2 of Schedule 1, Part 1, DPA 2018 (health or social care purposes; this condition does not require an appropriate policy document) — and for issuing correct Instructions. The parties note that this condition relies on the Processing being carried out under the responsibility of a health professional: AI output in the Service is draft documentation reviewed and adopted by the Controller's clinical staff, and the Controller shall maintain that review step in its use of the Service.

5.2 The Controller shall without undue delay inform the Processor of changes to the Processing which affect the Processor's obligations under Data Protection Legislation.

5.3 The Controller is responsible for informing Data Subjects about the Processing, for upholding Data Subjects' rights, and for every other measure incumbent on the Controller under Data Protection Legislation, including carrying out a data protection impact assessment in accordance with Article 35 UK GDPR and the ICO's guidance on AI and data protection before the Processing begins.

6. UNDERTAKINGS OF THE PROCESSOR

6.1 The Processor undertakes to carry out the Processing only in accordance with this DPA and for the specific purposes stated in the Instructions, to comply with Data Protection Legislation, and to keep itself informed of applicable law in this area.

6.2 The Processor shall take measures to protect the Personal Data against all forms of Processing incompatible with this DPA, the Instructions and Data Protection Legislation.

6.3 The Processor shall ensure that all natural persons working under its direction comply with this DPA and the Instructions, and that they are informed of relevant Data Protection Legislation.

6.4 The Processor shall, at the Controller's request, assist the Controller in ensuring compliance with Articles 32–36 UK GDPR and in responding to requests from Data Subjects exercising their rights under Chapter III UK GDPR, taking into account the nature of the Processing and the information available to the Processor. Without being asked, the Processor shall make available to the Controller a data protection impact assessment input pack describing the AI processing, its risks and the safeguards implemented, for use in the Controller's assessment under Article 35 UK GDPR.

6.5 If the Processor considers an Instruction to be unclear, contrary to Data Protection Legislation, or absent, and new or supplementary Instructions are necessary, it shall without delay inform the Controller, temporarily suspend the Processing and await new Instructions, unless the parties agree otherwise.

6.6 If the Controller provides new or amended Instructions, the Processor shall, without undue delay from receipt, notify the Controller whether implementing them entails changed costs.

6.7 The Processor shall **never use Personal Data processed under this DPA for training, further development or improvement of AI models**, whether its own or those of any third party. For the avoidance of doubt, this prohibition is absolute and applies regardless of any anonymisation or aggregation.

6.8 If the Processor is required by law, or by a binding order of a court or authority, to disclose Personal Data, it shall — unless prohibited by law from doing so — notify the Controller before disclosure, limit the disclosure to the minimum required, and inform the Controller of what was disclosed. Such compelled disclosure is not a breach of this DPA and does not extend the permitted purposes in section 2 or clause 6.7.

7. SECURITY MEASURES

7.1 The Processor shall implement all appropriate technical and organisational measures required by Data Protection Legislation to prevent Personal Data Breaches, by ensuring that the Processing meets the requirements of the UK GDPR and that the rights of Data Subjects are protected.

7.2 The Processor shall on an ongoing basis ensure that the technical and organisational security of the Processing provides an appropriate level of confidentiality, integrity, availability and resilience.

7.3 Additional or amended protection requirements from the Controller after signature shall be treated as new Instructions under this DPA.

7.4 The Processor shall, through access-control systems, give access to the Personal Data only to natural persons working under the Processor's direction who need access to perform their duties.

7.5 The Processor undertakes to continuously Log access to the Personal Data to the extent required by the Instruction. Logs shall be retained for the period stated in the Instruction (Annex 1 §6) and may not be deleted earlier; absent a stated period, logs may be deleted no earlier than five (5) years after the Logging event. Logs shall be subject to the necessary safeguards in accordance with Data Protection Legislation.

7.6 The Processor shall systematically test, assess and evaluate the effectiveness of the technical and organisational measures that ensure the security of the Processing.

8. CONFIDENTIALITY

8.1 The Processor and all natural persons working under its direction shall observe both confidentiality and — in respect of patient information — the common law duty of confidentiality when carrying out the Processing. Where the Caldicott principles apply to the Controller's practice, the Processor shall reasonably cooperate with the Controller's Caldicott governance. The Personal Data may not be used or disclosed for other purposes, directly or indirectly, unless otherwise agreed.

8.2 The Processor shall ensure that all natural persons working under its direction who take part in the Processing are bound by a confidentiality undertaking, unless they are already subject to a statutory duty of confidentiality. The Processor shall also ensure that confidentiality agreements exist with each Sub-processor and corresponding undertakings for the Sub-processor's personnel.

8.3 The Processor shall promptly notify the Controller of any contact with the Information Commissioner's Office (ICO) concerning the Processing. The Processor is not entitled to represent the Controller or act on the Controller's behalf towards the ICO in matters concerning the Processing.

8.4 If a Data Subject, the ICO or a third party requests information from the Processor concerning the Processing, the Processor shall refer the matter to the Controller. Information about the Processing may not be disclosed without the Controller's written consent unless disclosure is required by law. The Processor shall assist in conveying information covered by such consent or legal requirement.

9. REVIEW, SUPERVISION AND AUDIT

9.1 The Processor shall, without undue delay and as part of its guarantees under Article 28(1) UK GDPR, on request demonstrate to the Controller the technical and organisational measures used to meet the requirements of this DPA and Article 28(3)(h) UK GDPR.

9.2 The Processor shall at least once per year review the security of the Processing through a self-assessment to verify compliance with this DPA. The result shall be shared with the Controller on request.

9.3 The Controller may itself, or through a third party appointed by it (which may not be a competitor of the Processor), verify the Processor's compliance with this DPA, the Instructions and Data Protection Legislation. The Processor shall assist with documentation and access to premises, IT systems and other assets needed for the review. The Controller shall ensure that personnel conducting the review are bound by confidentiality by law or agreement.

9.4 As an alternative to 9.2–9.3, the Processor may offer other means of review, such as an audit performed by an independent third party (e.g. SOC 2 or ISO 27001 reports), Cyber Essentials or Cyber Essentials Plus certification, and a summary or attestation of a recent independent penetration test. The Controller is entitled, but not obliged, to accept such alternatives.

9.5 The Processor shall enable the ICO, or another authority with a legal right to it, to carry out supervision in accordance with applicable law, even where such supervision would otherwise conflict with this DPA.

9.6 The Processor shall secure for the Controller rights against each Sub-processor corresponding to all of the Controller's rights against the Processor under this section 9.

10. RECTIFICATION, ERASURE ETC.

10.1 Where the Controller has requested rectification or erasure due to the Processor's incorrect Processing, the Processor shall take the appropriate measure without undue delay and at the latest within thirty (30) days of receiving the necessary information. Where erasure is requested, the Processor may only Process the Personal Data concerned as part of the rectification/erasure process.

10.2 If the Processor takes technical or organisational measures (e.g. upgrades or troubleshooting) that may affect the Processing, the Controller shall be informed in writing in good time beforehand, in accordance with section 18.

11. PERSONAL DATA BREACHES

11.1 The Processor shall be able to restore availability of, and access to, the Personal Data within reasonable time following a physical or technical incident, in accordance with Article 32(1)(c) UK GDPR.

11.2 The Processor undertakes, taking into account the nature of the Processing and the information available to it, to assist the Controller in fulfilling the Controller's obligations in the event of a Personal Data Breach — including the Controller's notification obligation to the ICO (72 hours) and communication to affected Data Subjects — and, on request, to assist in investigating suspected unauthorised Processing or access.

11.3 Upon becoming aware of a Personal Data Breach, the Processor shall notify the Controller in writing without undue delay, and in any event within forty-eight (48) hours, and provide a written description of the breach, covering: its nature and, where possible, the categories and approximate number of Data Subjects and records concerned; the likely consequences; and the measures taken or proposed, including measures to mitigate adverse effects.

11.4 If it is not possible to provide the full description at once, it may be provided in phases without undue further delay.

12. SUB-PROCESSORS

12.1 The Processor may engage the Sub-processors listed in Annex 2.

12.2 The Processor shall enter into a written agreement with each Sub-processor imposing the same data protection obligations as those imposed on the Processor under this DPA, and shall engage only Sub-processors providing sufficient guarantees.

12.3 The Processor shall in its agreement with the Sub-processor ensure that the Controller may terminate the Sub-processor engagement and instruct the Sub-processor to delete or return the Personal Data if the Processor has ceased to exist in fact or in law or has become insolvent.

12.4 The Processor is fully liable to the Controller for the Sub-processors' Processing and shall promptly notify the Controller if a Sub-processor fails to fulfil its obligations.

12.5 The Processor may engage new Sub-processors and replace existing ones unless otherwise stated in the Instruction.

12.6 Before engaging or replacing a Sub-processor, the Processor shall verify its capacity to comply with Data Protection Legislation and give the Controller written notice of the Sub-processor's name,

registration number and seat; the types of data and categories of Data Subjects; and where the Personal Data will be Processed.

12.7 The Controller may object within thirty (30) days of such notice. On objection, the parties shall discuss in good faith, and the Processor may propose an alternative Sub-processor or a configuration that avoids the objected Sub-processor. If no solution is agreed within thirty (30) days of the objection, the Controller may terminate the part of the services that requires the objected Sub-processor in accordance with section 16.4.

12.8 The Processor shall maintain an accurate, current list of engaged Sub-processors — including country of Processing and types of Processing — and make it available to the Controller.

12.9 When the Processor ceases to use a Sub-processor it shall notify the Controller in writing and ensure that the Sub-processor deletes or returns the Personal Data.

12.10 On request, the Processor shall provide a copy of the agreement governing a Sub-processor's Processing and the list under 12.8.

13. LOCALISATION AND TRANSFERS TO THIRD COUNTRIES

13.1 The Processor shall ensure that the Personal Data is stored, and that serverless application processing is executed, within the UK/EEA at the locations listed in Annex 2, unless the parties agree otherwise. Request traffic to and from the application additionally passes, in transit and TLS-encrypted, through the content delivery network of the hosting platform (Vercel), whose edge locations are not region-pinned; no Personal Data is persisted there (see Annex 2). The parties note that the EEA is covered by UK adequacy regulations, so the flow of Personal Data from the UK to the Processor's EEA infrastructure requires no additional transfer safeguards. Where a Sub-processor's corporate group includes entities established outside the UK/EEA, the hosting locations in Annex 2 apply, and any resulting third-country transfer or access scenario is governed by clauses 13.2–13.3 and the safeguards documented per Sub-processor.

13.2 The Processor may transfer Personal Data to a Third Country for Processing (e.g. service, support, maintenance, development or operations) only with the Controller's prior written approval and documented Instructions for that purpose.

13.3 Any transfer under 13.2 may only take place if compatible with Data Protection Legislation — including, where required, an International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses — and with the requirements of this DPA and the Instructions.

14. LIABILITY FOR DAMAGE IN CONNECTION WITH PROCESSING

14.1 Compensation payable to a Data Subject, by final judgment or settlement, for damage caused by breach of this DPA, the Instructions and/or Data Protection Legislation shall be governed by Article 82 UK GDPR and sections 168–169 DPA 2018.

14.2 Administrative fines under Article 83 UK GDPR or penalties under the DPA 2018 shall be borne by the party on whom they are imposed.

14.3 If a party becomes aware of circumstances that may cause damage to the other party, it shall without undue delay inform the other party and actively work with it to prevent and minimise the damage.

14.4 Notwithstanding the Main Agreement, clauses 14.1 and 14.2 prevail over other rules on allocation of claims between the parties in respect of the Processing.

14.5 The Processor shall indemnify the Controller against losses, claims and regulatory penalties incurred by the Controller to the extent caused by the Processor's breach of this DPA or unlawful Processing, up to an aggregate amount equal to twelve (12) months' fees paid under the Main Agreement. This cap does not apply to breaches of section 8 (confidentiality).

14.6 The Processor shall maintain professional indemnity insurance and cyber liability insurance, each with a minimum cover of £2,000,000 per claim, and shall provide certificates of insurance on request.

15. TERM AND TERMINATION

15.1 This DPA applies from acceptance under section 22 and remains in force for as long as the Main Agreement is in force. It cannot be terminated separately while the Main Agreement continues, and it terminates automatically when the Main Agreement ends. Sections 8 (confidentiality), 14 (liability) and 17 (measures upon termination) survive termination.

16. AMENDMENTS AND TERMINATION WITH IMMEDIATE EFFECT

16.1 Either party may call for renegotiation if the other party's ownership changes materially or if applicable law, or its interpretation, changes in a way material to the Processing. Calling for renegotiation does not suspend the DPA.

16.2 Additions and amendments shall be in writing and signed by both parties.

16.3 If a party becomes aware that the other party is acting in breach of this DPA and/or the Instructions, it shall notify the other party without delay and may suspend performance until the breach has ceased and the explanation has been accepted.

16.4 If the Controller objects to a new Sub-processor under 12.7 and no solution is agreed within the period stated there, the Controller may terminate the affected part of the services — or, where the objected Sub-processor is essential to the service as a whole, the Main Agreement and this DPA — with thirty (30) days' notice.

17. MEASURES UPON TERMINATION

17.1 Upon termination, the Processor shall without undue delay, at the Controller's choice, either delete — and certify deletion of — or return: all Personal Data Processed on the Controller's behalf, and all associated information such as Logs, Instructions, system solutions, descriptions and other documents received through the exchange of information under this DPA.

17.2 On return, the Processor shall also delete existing copies.

17.3 The obligation to delete or return does not apply where retention is required by UK law.

17.4 Returned data shall be provided in a commonly used, standardised format unless otherwise agreed.

17.5 Until deletion or return, the Processor shall continue to comply with this DPA.

17.6 Return or deletion shall be completed within thirty (30) calendar days of termination unless otherwise stated in the Instruction. Processing thereafter constitutes unauthorised Processing.

17.7 The confidentiality provisions in section 8 survive termination of this DPA.

18. NOTICES

18.1 Notices concerning this DPA and its administration, including termination, shall be sent by e-mail (or as otherwise agreed) to each party's DPA contact person.

18.2 Notices concerning the parties' data protection cooperation shall be sent to each party's data protection contact person.

18.3 A notice is deemed received no later than one (1) business day after sending.

19. CONTACT PERSONS

Each party shall appoint a contact person for this DPA and a contact person for data protection cooperation (section 1).

20. RESPONSIBILITY FOR PARTY DETAILS

Each party is responsible for keeping the details in section 1 current and correct, and shall notify the other party of changes in accordance with section 18.1.

21. GOVERNING LAW AND DISPUTES

This DPA is governed by the laws of England and Wales, excluding its conflict-of-law rules. Disputes arising out of this DPA shall be settled by the courts of England and Wales.

22. EXECUTION OF THIS DPA

22.1 This DPA is entered into electronically. The Controller accepts the agreement by ticking the acceptance checkbox for the Data Processing Agreement when registering in the Service. Upon acceptance, the agreement version, the timestamp, the accepting user and a cryptographic checksum (SHA-256) of the document are recorded, which together constitute the parties' entry into this agreement. No further signature is required.

22.2 The individual ticking the acceptance checkbox represents and warrants that they are authorised to enter into this DPA on behalf of the Controller. References to the Controller include the organisation on whose behalf the account is registered.

ANNEX 1 — THE CONTROLLER'S INSTRUCTION FOR THE PROCESSING OF PERSONAL DATA

1. Purpose, subject matter and nature

1a. Subject matter: providing the Edith Care service to the Controller's users (assessors, psychologists and administrators), including account management, login, permissions, document upload, transcription of clinical conversations, AI-assisted compilation of assessment documentation and management of assessment records.

1b. Purpose: enabling AI-assisted documentation and compilation in neurodevelopmental assessments (autism, ADHD, combined assessments), and administrative management of users and permissions within the Controller's care services.

1c. Nature of the Processing: collection (via users/document upload), recording, storage, structuring, transcription, AI-assisted analysis and compilation, access, use, reporting, troubleshooting/support, security logging, deletion/return upon termination.

2. Types of Personal Data

- Account data: name, e-mail, user ID, role (assessor/psychologist/admin), practice name and team
- Technical data: IP address, device/browser information (user agent), logs of logins and admin actions
- Health data (special category data, Article 9 UK GDPR): uploaded assessment documents, transcribed clinical conversations, AI-generated compilations, assessment material and results; assessment administration (patient cases, templates, status, document flows)
- Messages/support: support tickets and related communication
- AI-assisted analysis: AI-generated compilations, assessment drafts and document drafts linked to patient cases

The Processing by its nature concerns special category data (health data). The lawful basis is provided by the Controller under Article 9(2)(h) UK GDPR together with paragraph 2 of Schedule 1, Part 1, DPA 2018.

3. Categories of Data Subjects

- Patients (persons undergoing neurodevelopmental assessment)
- Clinical staff (assessors, psychologists, administrators)
- Administrators (management/IT)

4. Special handling requirements — retention

- Account and assessment data: retained for the term of the Main Agreement and deleted/returned within 30 days of termination (unless the Controller requests export). For clarity, the assessment data the Processor persists on the Controller's behalf includes report drafts and generated report documents, uploaded source documents, transcripts of clinical conversations, patient test invitations and answers, and document version history.
- Clinical record-keeping: the Controller's statutory record-keeping obligations remain with the Controller and its clinical record system; content held by the Processor is processed as draft/working documentation on the Controller's behalf and is deleted per this section, not retained as the clinical record
- Support tickets: 24 months (traceability), then deleted/anonymised
- Database and platform backups: rolling, maximum 35 days
- Raw audio recording backup chunks (uploaded only when realtime transcription is unavailable): platform-enforced lifecycle deletion approximately 7–8 days after creation
- Logs: 12 months

5. Technical and organisational security measures

Technical: TLS/HTTPS in transit (frontend and backend), enforced HTTPS + HSTS and secure cookies; encrypted database connections (TLS required); encryption at rest via the Azure platform (AES-256) for database, object storage and backups; least-privilege access control, separate admin accounts, MFA

for administrative accounts and strong authentication for end users (e-mail/password with TOTP multi-factor authentication); logging/traceability via platform and application logs, protected against unauthorised access; vulnerability and patch management (Azure platform patched by Microsoft; application/dependencies patched by Edith Care); backup and restore procedures via Azure Sweden Central.

Organisational: permission governance including onboarding/offboarding and regular access reviews; confidentiality undertakings for personnel (and relevant subcontractors) plus basic security training; incident process including reporting to the Controller without undue delay; annual self-assessment/review of relevant security procedures.

6. Logging requirements

Log: logins, permission changes, admin actions, error/incident events, and — as metadata-only entries (user, timestamp, action, resource identifiers; never content or patient-identifying free text) — access to and export of personal data, including report, document, transcript and test-answer read/download/export actions. Access to logs: designated admin/technical roles only. Retention: 12 months.

7. Localisation and Third Country transfers

Primary persistent application data (database, object storage, backups) is processed in Sweden (Azure Sweden Central; data centres in Gävle/Sandviken and Staffanstorp). Certain ancillary processing (telemetry, error monitoring, transactional e-mail, application hosting) takes place at the other UK/EEA locations listed in Annex 2. Absent instructions on Third Country transfer in this Instruction, the Processor has no right to make such a transfer. Personal Data may not be transferred to a Third Country without the Controller's written approval and documented instruction.

8. Duration

For the term of the Main Agreement, and otherwise per section 17 (measures upon termination).

9. Other instructions

Speech-to-text transcription for the Controller's tenancy is performed by Azure Speech Services (Sweden Central), and AI text processing by Azure OpenAI Service (Sweden Central), each as listed in Annex 2. Annex 2 is exhaustive: the Processor shall not use any speech-to-text or AI processing provider not listed in Annex 2 for the Controller's Personal Data, and any addition or replacement of such a provider constitutes a change of Sub-processors subject to the notice and objection process in section 12.

ANNEX 2 — LIST OF APPROVED SUB-PROCESSORS

All listed hosting locations for storage and serverless processing are within the UK/EEA; as set out in clause 13.1, request traffic additionally transits the hosting platform's TLS-encrypted, non-region-pinned edge network without persistence. Several suppliers have contracting or parent entities established outside the UK/EEA — per-supplier verification of contracting entity and access locations is documented in the Processor's supplier verification records, available to the Controller on request. Adding any Sub-processor with a hosting location outside the UK/EEA triggers the transfer-safeguard analysis in section 13 and the notice/objection process in section 12.

Sub-processor	Location of Personal Data	Data types	Purpose	Retention	Notes
Microsoft Corporation (Azure Database for PostgreSQL)	Sweden (EEA) — Azure Sweden Central	All data: account data, assessment data, health data (Art 9), technical logs	Primary database for all persistent storage	Term of agreement + Instruction (deletion/return on termination)	Microsoft DPA applies
Microsoft Corporation (Azure OpenAI Service)	Sweden (EEA) — Azure Sweden Central	Clinical text (prompts/responses); no storage — processed in real time	AI text processing: generation of assessment documentation drafts	No persistent storage; zero data retention	Microsoft commitment: no customer data used for model training
Microsoft Corporation (Azure Speech Services)	Sweden (EEA) — Azure Sweden Central	Audio recordings (clinician–patient conversations); no persistent storage	Transcription of clinical conversations (speech-to-text)	No persistent storage; audio deleted after transcription	Zero data retention; Microsoft DPA applies
Microsoft Corporation (Azure Blob Storage)	Sweden (EEA) — Azure Sweden Central	Uploaded assessment/source documents (may contain Art 9 health data), template files/attachments, raw audio backup chunks (generated report content is stored in the database, not in object storage)	File/object storage for uploaded evidence, templates and conditional audio backup	Documents/templates: term of agreement + Instruction. Raw audio backup chunks: lifecycle-deleted ~7–8 days after creation	Encrypted at rest (AES-256)
Microsoft Corporation (Azure AI Document Intelligence)	Sweden (EEA) — Azure Sweden Central	Uploaded assessment documents/PDFs (may contain Art 9 health data)	OCR — text extraction from uploaded documents	No persistent storage; extracted text never logged	Microsoft DPA applies
PostHog Inc.	EU (Frankfurt, Germany)	Pseudonymous product telemetry: staff user ID, role, organisation ID, and pseudonymous report/case and test-invitation identifiers, plus counts, enums and durations; never clinical content, e-mail addresses, test answers or scores, prompts, or transcript/report text	Product analytics	Per PostHog retention policy (~90 days session data)	EU hosting; identifiers are metadata-only references — patient-side test events are keyed by invitation ID, never patient e-mail

Sub-processor	Location of Personal Data	Data types	Purpose	Retention	Notes
Langfuse GmbH	EU (Frankfurt, Germany)	Pseudonymous operational metadata in production: report/case identifiers, latency, token counts, model version, error codes; prompts, responses and patient content are not recorded in production	AI observability and quality assurance	Per Langfuse retention policy	EU hosting; production traces carry identifiers and metrics only
Functional Software, Inc. (Sentry)	EU (Frankfurt, Germany) — Sentry EU region	Technical error data: messages, stack traces, release/environment; no IP/cookies/PII (sendDefaultPii: false); no patient data	Error monitoring and stability	Per Sentry retention policy (~90 days)	Server-side scrubbing (beforeSend) keeps patient data out of error payloads
Resend, Inc.	EEA — Ireland (AWS eu-west-1)	Staff account data in transactional e-mail (name, e-mail, organisation) and, where the patient self-report test feature is used, patient contact/link-delivery data (patient e-mail address, test invitation links, one-time codes) and the optional clinician-entered invitation message; never test answers, report content or transcripts	Transactional e-mail (activation, invitations, password reset, patient test invitations/codes)	Per Resend retention policy	Verified sender domain in EU region; clinicians are responsible for not placing clinical content in the free-text invitation message
Vercel Inc.	Serverless function execution: Sweden (Stockholm, eu-north-1/arn1 — sole enabled Function Region, verified 2026-07-12). Request transit additionally passes Vercel's edge	Application traffic in transit (may include Art 9 health data in API calls); anonymous web telemetry	Application hosting/operations (serverless functions)	No persistent storage of patient data; data in transit/memory only	Persistent patient data resides in Azure Sweden Central; the localisation commitment covers function execution and storage, not transient encrypted network routing

Sub-processor	Location of Personal Data	Data types	Purpose	Retention	Notes
	network (TLS-encrypted; not region-pinned, as with any CDN-fronted platform)				

Last updated: 2026-07-12 (mirrors the Swedish Bilaga 2 as signed).