dentio.

Data Processing Agreement (DPA)

Last updated: 3 March 2026

Norrtullsgatan 6, 11329 Stockholm

Product: Dentio Practice Automation System

Dentio AB
org nr. 559498-5136

dentio.

Preamble

A. This Data Processing Agreement ("**DPA**") is entered into by and between the dental clinic or organization below (the "**Controller**" or "**Customer**") and Dentio AB (org.nr 559498-5136), Norrtullsgatan 2, 113 29 Stockholm, Sweden ("**Dentio**", "**Processor**", "**we**" or "**us**").

B. The Parties have entered into a separate software-subscription contract or terms of service (the "**Service Agreement**") under which Dentio provides AI-supported administrative tools for dental professionals to the Customer. In the course of providing the Services, Dentio will Process Personal Data on behalf of the Controller.

C. This DPA sets out the rights and obligations of the Parties with respect to such Processing, in accordance with Article 28 GDPR.

D. This DPA shall form an integral part of, and is incorporated by reference into, the Service Agreement. In the event of any conflict between this DPA and the Service Agreement, the provisions of this DPA shall prevail to the extent of the conflict, unless the Parties expressly agree otherwise in writing.

E. Capitalised terms not otherwise defined herein shall have the meanings given to them in the GDPR or, where relevant, in the Service Agreement.

F. The Parties expressly acknowledge and agree that this DPA does not establish a joint controllership arrangement under Article 26 GDPR. Each Party remains solely responsible for its own compliance with Applicable Law in respect of its separate processing activities. Dentio processes Personal Data solely on behalf of and under the documented Instructions of the Controller. Dentio does not engage in automated decision-making with legal or similarly significant effects on Data Subjects.

Parties & Contact Details

Role	Entity / Contact	Details
Controller	*[Clinic legal name]*	Address: *[Clinic address]*
		Reg./VAT no.: *[insert number]*
		Head clinician: [Name] Contact: *[Data-protection contact]*
Processor	**Dentio AB**	Org.nr 559498-5136
		Norrtullsgatan 6, 113 29 Stockholm, Sweden
		CEO: **Elias Afrasiabi**
		DPO: **Jonathan Ahrlind**
		Privacy and 24 h Incident mailbox: **dpo@dentio.io**

0 Structure and Interpretation

0.1 Integral Documents

This DPA consists of the main body and the following annexes:

- Annex 1 – Detailed Instructions for Processing
- Annex 2 – Technical and Organisational Measures (TOMs)
- Annex 3 – Approved Sub-Processors

0.2 Headings and References

Clause headings are for convenience only and do not affect interpretation. References to Articles are to those of the GDPR unless otherwise stated.

0.3 Incorporation of Law

References to any statute or statutory provision include any modification, extension or re-enactment thereof.

0.4 No Waiver

Failure or delay by either Party in exercising any right under this DPA shall not constitute a waiver of that right.

0.5 Severability

If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

0.6 Order of Precedence

In the event of any conflict between the provisions of this DPA and the Service Agreement, the provisions of this DPA shall prevail with respect to data protection matters. In the event of conflict between the main body of this DPA and any Annex, the main body shall prevail unless the Annex expressly states otherwise.

1 Definitions

1.1 Statutory terms

Capitalised terms that are defined in Applicable Law—including Controller, Processor, Personal Data, Processing, and Personal-Data Breach—have the same meaning in this DPA and are not restated here.

1.2 Contract-specific terms

Term	Meaning
Applicable Law	Any European Union or Member-State statute, regulation or binding decision that governs the Processing of Personal Data under this DPA.
Service Agreement	Has the meaning set out in preamble B.
Approved Purpose	The Processing strictly necessary to deliver the Services as described in Annex 1 or as otherwise documented in writing by the Controller.
Authorised Territory	The European Union (“EU”) and the European Economic Area (“EEA”) and any country recognised by the European Commission as providing an adequate level of protection under GDPR Art 45.
Approved Sub-Processor	A third-party processor listed in Annex 3, as amended in accordance with Section 4.
Instruction	A written instruction issued by the Controller that specifies how Dentio shall Process Personal Data; initial Instructions are set out in Annex 1.
Technical and Organisational Measures (“TOMs”)	The security controls implemented by Dentio and detailed in Annex 2.
Confidential Information	Non-public information disclosed by one Party to the other in connection with the Service Agreement or this DPA, subject to Section 11.
Personal Data Breach	The meaning given in Article 4(12) GDPR, being a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.
Data Subject	An identified or identifiable natural person whose Personal Data is Processed under this DPA, including but not limited to patients of the Controller.
Service Data	Aggregated and de-identified data relating to the use, support, and operation of the Services, collected by Dentio for its own purposes including analytics, security monitoring, and product improvement. Service Data contains no identifiable patient information.

2 Roles and General Obligations

2.1 Allocation of Roles

The Controller determines the purposes and means of Processing; Dentio acts solely as a Processor based on the Controller's documented Instructions (Art 4(7) & (8) GDPR).

2.2 Obligations of the Controller (Customer)

2.2.1 Documented Instructions

The Controller shall provide Dentio with documented Instructions for the Processing of Personal Data. Initial Instructions are set out in Annex 1, and any subsequent updates must be provided in writing, including by e-mail. The Controller is responsible for ensuring that all Instructions comply with Applicable Law.

2.2.2 Lawful Basis

The Controller shall ensure that a valid legal basis exists for all Processing of Personal Data under this DPA. Depending on the nature of the Processing, this may include Article 6(1)(b) GDPR where Processing is necessary for the performance of a contract with the Data Subject, Article 6(1)(c) where Processing is required to comply with a legal obligation such as healthcare record-keeping requirements, or Article 6(1)(f) where Processing is necessary for the purposes of legitimate interests. For special category data, including health data, the Controller shall ensure an appropriate legal basis exists under Article 9(2), which in the context of healthcare services will typically be Article 9(2)(h) concerning the provision of health or social care.

2.2.3 Transparency

The Controller shall inform Data Subjects, including patients and any other individuals whose Personal Data is processed, of the Processing in accordance with Articles 13 and 14 GDPR. This information shall be provided at the time Personal Data is collected and shall include clear notice that AI-assisted transcription and documentation tools are used in the provision of dental services.

2.2.4 Consent

Where the legal basis for Processing is consent, the Controller shall ensure that valid, informed, specific, and freely given consent has been obtained from Data Subjects prior to Processing. This applies in particular to the audio recording of clinical consultations and the use of AI tools to generate clinical documentation. The Controller shall maintain records of all consents obtained and make such records available to Dentio upon reasonable request.

2.2.5 Data Accuracy

The Controller shall ensure that all Personal Data provided to Dentio is accurate, complete, and kept up to date, and shall promptly notify Dentio of any corrections or updates required.

2.2.6 Supervision

The Controller shall supervise the Processing of Personal Data under this DPA throughout its duration. This supervision includes verifying, both before Processing begins and periodically thereafter, that Dentio complies with its obligations under this DPA and Applicable Law. The Controller shall conduct or commission audits and inspections in accordance with Section 9, and shall review and either approve or object to new Sub-Processors in accordance with Section 4. The Controller shall promptly notify Dentio of any Data Subject requests, complaints, or regulatory inquiries relating to the Processing.

2.2.7 AI Content Verification

The Controller shall ensure that clinicians and other authorised personnel using the Services review and verify all AI-generated content before such content is entered into patient records or relied upon for clinical purposes. The Controller shall take any other supervisory action required of a data controller under Applicable Law.

2.2.8 Healthcare Compliance

The Controller shall ensure compliance with all applicable healthcare-specific laws and regulations. In Sweden, this includes Patientdatalagen (2008:355), Patientsäkerhetslagen (2010:659), the regulations and general guidance issued by Socialstyrelsen under HSLF-FS concerning medical records, any sector-specific guidance issued by Integritetsskyddsmyndigheten (IMY), and applicable professional codes of conduct for dental practitioners.

2.2.9 Staff Training

The Controller shall ensure that all personnel authorised to use the Services receive appropriate training on data protection principles and obligations, the proper use of Dentio's AI-assisted tools, the requirement to review and verify AI-generated content before clinical use, and the procedures for reporting data protection incidents.

2.3 Obligations of the Processor (Dentio)

2.3.1 Processing Limitations

Dentio shall Process Personal Data only for the Approved Purpose and only in accordance with the Controller's documented Instructions. If Dentio is required by Union or Member State law to Process Personal Data for any other purpose, Dentio shall inform the Controller of that legal requirement before the Processing takes place, unless the relevant law prohibits such disclosure on important grounds of public interest.

2.3.2 Instruction Compliance

If Dentio considers that an Instruction from the Controller infringes the GDPR or any other Union or Member State data protection provision, Dentio shall immediately notify the Controller and may suspend the relevant Processing until the Instruction is clarified or withdrawn.

2.3.3 Confidentiality

Dentio shall maintain the confidentiality of all Personal Data processed under this DPA. Dentio shall ensure that all personnel authorised to Process Personal Data have committed themselves to confidentiality under written non-disclosure agreements or are subject to an appropriate statutory obligation of confidentiality.

2.3.4 Personnel Training

Dentio shall ensure that personnel authorised to Process Personal Data receive appropriate training in data protection principles and practices, both upon commencement of their duties and periodically thereafter, and that training completion is documented.

2.3.5 Security Measures

Dentio shall implement and maintain the technical and organisational security measures set out in Annex 2, and shall regularly review and update these measures to ensure they remain appropriate to the risks presented by the Processing, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the Processing.

2.3.6 Data Subject Rights

Dentio shall assist the Controller in responding to requests from Data Subjects exercising their rights under Chapter III of the GDPR, in accordance with Section 7 of this DPA. Taking into account the nature of the Processing and the information available to Dentio, Dentio shall provide such assistance as is reasonably necessary to enable the Controller to comply with its obligations to Data Subjects.

2.3.7 Compliance Assistance

Dentio shall assist the Controller, upon request and at the Controller's expense, in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR. This assistance shall include assistance with security of processing (Article 32), notification of Personal Data Breaches to the supervisory authority (Article 33), communication of Personal Data Breaches to Data Subjects (Article 34), data protection impact assessments (Article 35), and prior consultation with the supervisory authority (Article 36).

2.3.8 Audit Support

Dentio shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and in this DPA. Dentio shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, in accordance with Section 9 of this DPA.

2.3.9 Breach Notification

Dentio shall notify the Controller of any Personal Data Breach without undue delay in accordance with Section 6 of this DPA, and shall provide the Controller with such information and assistance as is necessary to enable the Controller to comply with its own breach notification obligations under the GDPR.

2.3.10 Data Deletion

Upon termination of the Services or this DPA, whichever occurs first, Dentio shall, at the choice of the Controller, delete or return all Personal Data to the Controller in accordance with Section 8 of this DPA, and shall delete all existing copies of Personal Data unless Union or Member State law requires further storage. Dentio shall certify the deletion in writing upon request.

2.4 Instruction Refusal

Dentio may refuse, suspend, or propose commercially reasonable alternatives to any Instruction it reasonably believes would breach this DPA, Applicable Law, or materially compromise the security, confidentiality, availability, or performance of the Services.

2.5 Instructions Outside Scope

If Dentio considers an Instruction to infringe Applicable Law, it will promptly inform the Controller and may suspend the Processing of Personal Data until the Instruction is clarified.

If the Controller provides additional instructions beyond what is expressly stated in this DPA and in the initial Instructions set out in Annex 1, Dentio is entitled to compensation for costs and additional work performed in order to comply with such instructions.

2.6 Data Protection by Design and Default

Dentio shall, with regard to its tools, products, applications, and services, apply the principles of data protection by design and data protection by default in accordance with Article 25 GDPR. This means that Dentio shall implement appropriate technical and organisational measures designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the Processing. Dentio shall further ensure that, by default, only Personal Data which is necessary for each specific purpose of the Processing is collected, stored, and otherwise processed, and that Personal Data is not made accessible to an indefinite number of persons without the individual's intervention.

2.7 Prohibited Data Categories

The Controller shall not provide to Dentio any Personal Data beyond that which is strictly necessary for the provision of dental services. Accidental capture of such categories during a recorded clinical consultation is permitted to the extent it is unavoidable and clinically relevant. Such incidental data is subject to the same security controls and retention rules described in this DPA.

3 Approved Locations for Processing and International Transfers

3.1 Authorised Territory

All Processing of Personal Data by Dentio or an Approved Sub-Processor shall take place exclusively within the Authorised Territory and Personal Data shall remain at rest in the Authorised Territory for the entire data life-cycle. As at the Effective Date, Personal Data will be Processed at the locations set out in Annex 3. No other hosting locations are authorised unless and until Annex 3 is updated in accordance with Section 4.

3.2 International Transfers of Personal Data

Dentio shall not transfer Personal Data to, or allow access to Personal Data from, any location outside the Authorised Territory.

All AI inference, storage, and processing are performed exclusively within EU regions. Dentio implements double-encryption with keys separated across independent services. Any residual risk related to access by non-EU headquartered vendors is assessed and mitigated through contractual, organisational, and technical controls.

For the avoidance of doubt, encrypted Internet transit through networks located outside the EEA does not constitute a transfer of Personal Data where the data is neither stored nor decrypted outside the Authorised Territory.

Technical support access from locations outside the Authorised Territory is prohibited unless expressly authorised in writing by the Controller and subject to appropriate safeguards under Chapter V GDPR.

Any Sub-Processor access to Personal Data must occur exclusively from within the Authorised Territory.

3.3 Support Access

Operational staff with production access are based in Sweden or another EU/EEA Member State. Remote connections originate only from the EU/EEA; any exception requires the Controller's prior written approval.

3.4 Future Cross-Border Transfers

If a transfer of Personal Data to a location outside the Authorised Territory becomes strictly necessary, Dentio will:

a) give the Controller 30 days' prior written notice; b) implement the EU Standard Contractual Clauses and any required supplementary measures; c) provide a documented Transfer Impact Assessment; and d) honour the Controller's right to object to the transfer.

3.5 Evidence of Compliance

Dentio maintains up-to-date data-flow diagrams and region-lock logs and will provide copies on request during an audit.

3.6 Disclosure to Public Authorities

If Dentio receives a legally binding request from any public authority, including law enforcement agencies or intelligence services, to disclose Personal Data processed on behalf of the Controller, Dentio shall immediately notify the Controller of such request unless legally prohibited from doing so.

Dentio shall challenge any such request where there are reasonable grounds to consider it unlawful, and shall exhaust all available remedies and appeals before making any disclosure.

Where disclosure is ultimately required, Dentio shall provide only the minimum amount of Personal Data legally necessary to comply with the request.

Dentio shall document all disclosures made in response to public authority requests and make such documentation available to the Controller upon request.

4 Sub-Processors

4.1 Approved Sub-Processors

The Controller hereby grants Dentio a general written authorisation, within the meaning of Article 28(2) GDPR, to engage the third-party processors identified in Annex 3 (Approved Sub-Processors). Each entity in Annex 3 has been vetted by Dentio for technical competence, financial stability and GDPR compliance and is bound by a written agreement imposing obligations no less protective than those set out in this DPA.

4.2 On-boarding Procedure for New Sub-Processors

a) **Prior notice.** Dentio shall provide the Controller with thirty (30) calendar-days' prior written notice before authorising any additional or replacement Sub-Processor (the "Notice Period"). The notice will include the Sub-Processor's full legal name, corporate seat, processing location(s), description of services and categories of Personal Data involved.

b) **Right to object.** During the Notice Period the Controller may object on reasonable, documented grounds relating to data protection (e.g. the proposed provider lacks adequate security certifications or would entail a restricted international transfer).

c) **Resolution of objection.** If an objection is raised, Dentio may at its sole discretion:

- (i) cancel or delay the intended engagement;
- (ii) propose a mitigation plan addressing the stated grounds; or
- (iii) offer the Controller the option to suspend or terminate the portion of the Services that would involve the objected-to Sub-Processor.

4.3 Flow-Down of Obligations

Dentio shall ensure that every Sub-Processor contract imposes data-protection obligations equivalent to those in this DPA.

4.4 Due Diligence and Monitoring

Before on-boarding a Sub-Processor and at least annually thereafter, Dentio shall conduct and document a risk-based assessment of each Sub-Processor's security posture, certifications (e.g. ISO 27001, SOC 2 Type II) and incident history. Dentio will make a summary of such assessments available to the Controller upon request no more than once per contract year.

4.5 Liability

Dentio shall remain fully liable to the Controller for the performance of each Sub-Processor's obligations and for any acts or omissions of the Sub-Processor, as if they were Dentio's own acts or omissions (Article 28(4) GDPR).

4.6 Emergency Replacement

If Dentio must urgently replace a Sub-Processor to maintain Service availability or comply with law (e.g. provider insolvency, security breach), Dentio may do so without the 30-day Notice Period, provided that:

a) the Controller is informed as soon as reasonably practicable; b) the replacement provider meets or exceeds the security and compliance level of the predecessor; and c) the Controller retains a prompt right to object under Section 4.2(b) once informed.

4.7 Sub-Processor List

Annex 3 shall always reflect the current roster of Approved Sub-Processors. Dentio will publish the up-to-date Annex 3 within the Dentio admin console and include a changelog of all amendments for audit purposes.

5 Technical and Organisational Measures ("TOMs")

Dentio maintains a documented information security programme based on recognised industry best practices. The measures implemented by Dentio are set out in Annex 2 – Technical and Organisational Measures.

5.1 Governance and Risk Management

- Board-approved security policy reviewed annually
- Security steering group reporting to CEO/DPO
- Formal risk register with quarterly review cycles

5.2 Data Minimisation and Encryption

- AES-256 encryption at rest with Google-managed encryption keys
- TLS 1.2+ for all data in transit
- Audio stream chunked into six-second segments and erased immediately after transcription (≤ 24 h buffer)
- Transcript text automatically deleted after 30 days

5.3 Access Control and Authentication

- Role-based access with zero default staff permissions
- Production consoles protected by mandatory MFA

5.4 Segregation and Multi-Tenant Isolation

- Customer data isolated at schema level in Supabase; row-level security prevents cross-tenant reads
- Multi-region object buckets use identity-bound encryption keys

5.5 Resilience, Backup and Disaster Recovery

- Daily encrypted snapshots stored in a separate EU region, retained 30 days

5.6 Incident Response

- 24 × 7 on-call rotation
- Documented incident-response plan with post-incident root-cause analysis
- Controller notified within 24 h of confirmed Personal Data Breach

5.7 Testing and Audit

- Security controls tested before every production release (static code analysis, dependency scanning)
- Annual third-party penetration-test report summary provided to the Controller on request
- Audit cooperation as set out in Section 9

5.8 Adequacy of Measures

The Parties agree that these measures provide a level of security appropriate to the risk, consistent with Article 32 GDPR, taking account of the state of the art, implementation cost and the nature, scope and context of the Processing.

6 Personal Data Breach Notification and Management

6.1 Definition and Scope

A Personal Data Breach means any event that meets the definition in Article 4(12) GDPR and includes, without limitation, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed for the Controller.

6.2 Notification Timeline

Upon becoming aware that a Personal Data Breach has occurred, Dentio shall notify the Controller without undue delay and in any event within twenty-four (24) hours of becoming aware.

6.3 Notification Method and Point of Contact

Dentio will send the initial breach notice to:

a) the Controller Contact Person named in the Parties table; and b) the 24 h incident mailbox supplied by the Controller (if any), using encrypted e-mail.

6.4 Information to be Included

Dentio's initial notice—and any subsequent updates—shall contain, to the extent known at the time:

a) the nature of the incident; b) the categories and approximate number of Data Subjects affected; c) the categories and approximate number of Personal Data records affected; d) the likely consequences of the breach; e) the measures taken or proposed to mitigate its adverse effects; and f) the name and direct contact details of Dentio's DPO or incident lead.

If it is not possible to provide all of this information simultaneously, Dentio may supply it in phases without undue delay.

6.5 Mitigation and Remediation

Dentio shall promptly take all measures necessary to contain, eradicate and remedy the Personal Data Breach, including patching vulnerabilities, resetting credentials and restoring data from clean backups as required.

6.6 Cooperation with Controller Notifications

Dentio shall cooperate with and assist the Controller in meeting its obligations under Articles 33 and 34 GDPR. This includes:

a) providing reasonable assistance in preparing and submitting notifications of Personal Data Breaches to the Swedish Authority for Privacy Protection or other competent supervisory authority; b) drafting communications to affected Data Subjects where such communication is required under Article 34; and c) providing any additional information reasonably requested by the Controller to enable it to comply with its notification and communication obligations.

Dentio shall make relevant personnel available for consultation and shall respond to Controller requests for breach-related information within twenty-four hours during an active incident.

6.7 Costs

If the Personal Data Breach has been caused by the Controller, Dentio is entitled to compensation for costs and additional work performed related to the Personal Data Breach.

6.8 Customer Notification Obligations

If the Controller determines to notify any governmental entity, Data Subjects, the public, or others of a Personal Data Breach, and such notice directly or indirectly refers to or identifies Dentio, the Controller agrees to:

a) notify Dentio in writing in advance; and b) in good faith, consult with Dentio and consider any clarifications or corrections Dentio may reasonably recommend, provided such recommendations are consistent with Applicable Law.

7 Information and Rights of Data Subjects

7.1 Obligation to Inform Data Subjects

The Controller is solely responsible for furnishing Data Subjects with the information required by Articles 12–14 GDPR at the time Personal Data is collected.

7.2 Assistance with Data Subject Requests

Dentio shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible taking into account the nature of the Processing, for the fulfilment of the Controller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III GDPR.

These rights include:

a) the right of access (Article 15); b) the right to rectification (Article 16); c) the right to erasure (Article 17); d) the right to restriction of processing (Article 18); e) the right to data portability (Article 20); f) the right to object (Article 21); and g) rights related to automated individual decision-making (Article 22).

Dentio provides self-service tooling within the admin console to enable the Controller to respond to Data Subject requests efficiently. This includes functionality to:

- export session data in PDF format;
- delete individual sessions; and
- submit requests for bulk data export or bulk deletion.

Dentio shall respond to Controller requests for assistance with Data Subject rights within five (5) business days. Where the Controller indicates that a request is urgent due to regulatory deadlines or other time-sensitive circumstances, Dentio shall use reasonable efforts to respond within forty-eight (48) hours.

7.3 Requests Received Directly by Dentio

If a Data Subject contacts Dentio directly, Dentio shall forward these requests as soon as they are received to the Controller Contact Person and take no further action unless instructed in writing by the Controller.

7.4 Costs

Dentio reserves the right to charge the Controller for the reasonable administrative costs of assistance in connection with Data Subject requests. Dentio will notify the Controller before levying any such charge.

8 Data Retention and Deletion Policy

8.1 Purpose Limitation

Dentio retains Personal Data only for as long as is strictly necessary to accomplish the Approved Purpose specified in Annex 1, after which it is either securely deleted or irreversibly anonymised.

8.2 Standard Retention Schedule

Data Category	Processing Stage	Maximum Retention	Location and Protection	Deletion Method
Raw audio stream	During speech-to-text transcription	≤ 24 h buffer (FIFO)	Google Cloud Run ephemeral disk (EU)	GCP automatic deletion through memory deallocation
Full transcript and AI draft note	Post-transcription storage	30 days from upload	Supabase Postgres and object storage (encrypted at rest, EU)	SQL DELETE + object-lifecycle rule → secure overwrite; cryptographic erasure of KMS key

Notes:

a) All retention timers start at the moment of successful upload (or creation, for logs).

b) If a Controller issues an earlier deletion instruction, that instruction overrides the timer (see Section 8.3).

c) No raw consultation content is stored in any Dentio analytics dashboard; only counts, durations and error codes.

8.3 Controller-Initiated Deletion or Export

8.3.1 Self-Service Tooling

The Dentio admin console provides a "Delete session" button and buttons for PDF export of periodontal charts and odontograms for each recorded consultation. Export delivers a PDF via secure download link that expires in 24 hours.

8.3.2 Bulk Requests

The Controller may submit bulk deletion or export tickets to info@dentio.io. Dentio will complete such requests within five (5) business days unless a shorter timeframe is required by Applicable Law.

8.4 Automatic Deletion on Termination of Services

a) **Export window.** Upon termination of the Service Agreement (for any reason), the Controller has fourteen (14) calendar days to request a final structured export of remaining Personal Data.

b) **Hard-delete deadline.** If no request is made, Dentio will permanently delete all Personal Data thirty (30) calendar days after the effective termination date, retaining only anonymised metrics and security logs (which contain no raw patient data).

c) **Proof of destruction.** Dentio shall, upon written request, provide a digitally-signed Certificate of Deletion confirming the date, time, scope and method of destruction.

d) **Backup persistence.** Deleted data may persist in encrypted backups for up to thirty (30) days before being permanently removed in accordance with Section 8.7.

8.5 Secure Deletion Methods

Dentio's deletion processes employ cryptographic erasure by destroying the encryption key (primary method) and secure overwrite procedures where applicable.

8.6 Legal Holds and Statutory Retention

If Dentio is required by Union or Member State law to retain specific data beyond the periods above (e.g., court order, ongoing litigation), Dentio shall:

a) isolate the data from ongoing Processing;

b) notify the Controller of the legal basis and expected duration (unless legally prohibited); and

c) delete the data immediately after the legal retention obligation ceases.

8.7 Backups and Disaster Recovery Copies

Backups are encrypted using a separate, hierarchical KMS key. When source data is deleted, Dentio's backup lifecycle policy ensures corresponding backup objects are also purged within thirty (30) days.

9 Audit & Inspection Rights

9.1 Controller Right to Audit

The Controller (or an independent auditor it appoints) may audit Dentio's compliance with this DPA:

a) once per rolling twelve (12) month period; and

b) if a confirmed Personal Data Breach directly involving the Controller's data occurs.

9.2 Notice and Scope

Any audits performed by the Controller shall be subject to:

a) **Prior written notice:** thirty (30) days, or five (5) days in case of a Personal Data Breach-triggered audit.

b) **Scope of audit:** security controls, Sub-Processor contracts, and evidence of the TOMs in Annex 2.

c) **Method:** documentation review first; on-site or video audit only if documentation is insufficient.

9.3 Conditions for the Audit

a) Auditors must sign a confidentiality agreement and follow Dentio's safety procedures.

b) Audits must avoid disproportionate disruption to Dentio's operations and not access other customers' data.

c) Dentio may redact commercially sensitive information not relevant to the audit objective.

9.4 Third-Party Reports

ISO 27001 certificates, SOC 2 (Type II) reports, or equivalent third-party assessments may be used to satisfy the Controller's audit requirements.

9.5 Costs

Dentio shall bear its own internal costs incurred in connection with an audit. All external costs (e.g., travel, third-party audit firm) shall be borne by the Controller.

9.6 Follow-Up

Dentio will remediate any identified non-conformities without undue delay and provide the Controller with a written remediation plan and proof of completion.

9.7 Supervisory Authority Cooperation

If Dentio receives any request, inquiry, investigation notice, or other communication from the Swedish Authority for Privacy Protection (IMY) or any other competent supervisory authority relating to Personal Data processed under this DPA, Dentio shall:

a) notify the Controller immediately and in any event within forty-eight (48) hours of receipt, unless such notification is legally prohibited;

b) provide the Controller with copies of all relevant correspondence with the supervisory authority;

c) unless legally required to respond sooner, not respond substantively to the supervisory authority without first consulting the Controller regarding the proposed response; and

d) cooperate with the Controller in formulating and submitting responses to supervisory authority inquiries, and provide all reasonable assistance requested by the Controller in connection with any regulatory investigation or proceeding.

10 Liability and Indemnification

10.1 Mutual Responsibility

Each Party is liable for the damages it causes by breaching this DPA or Applicable Law.

10.2 Cap on Damages

Except for the exclusions in Section 10.3, each Party's aggregate liability arising out of or in connection with this DPA is limited to the total subscription fees paid (or payable) by the Controller to Dentio during the twelve (12) months immediately preceding the event giving rise to the claim.

10.3 Exclusions from the Cap

The limitation in Section 10.2 does not apply to:

a) wilful misconduct or gross negligence;

b) liability that cannot be limited under mandatory law (e.g., death or personal injury);

c) either Party's breach of its confidentiality obligations (Section 11);

d) Dentio's breach of Section 3 (unauthorised international transfers); and

e) Dentio's breach of Section 4 (unauthorised Sub-Processors).

10.4 Time Limits

Claims under this DPA must be brought within two (2) years after the claimant became aware of the event.

10.5 Customer Indemnity

The Controller shall defend, indemnify, and hold harmless Dentio from any third-party claim, regulatory investigation, fine, or reasonable legal cost arising from:

a) the Controller's Instructions or configurations that cause a breach;

b) the Controller's failure to secure a lawful basis or required consents;

c) the Controller's provision of Prohibited Data Categories to Dentio; or

d) any breach of this DPA or Applicable Law by the Controller.

Dentio shall provide prompt written notice and reasonable cooperation. The Controller may not settle any matter that admits fault on behalf of Dentio or imposes non-monetary obligations on Dentio without Dentio's prior written consent.

11 Confidentiality

11.1 Scope

"Confidential Information" includes all non-public information, in any form, disclosed by one Party ("Disclosing Party") to the other ("Receiving Party") in connection with the Service Agreement or this DPA—specifically patient data, security reports, pricing, business plans, and trade secrets.

11.2 Obligations of the Receiving Party

The Receiving Party shall:

a) use Confidential Information solely to perform rights or obligations under the Service Agreement and this DPA;

b) apply the same degree of care it uses to protect its own confidential information—not less than reasonable care;

c) disclose Confidential Information only to personnel (employees, contractors, Sub-Processors, auditors) who:

- have a strict "need-to-know"; and
- are bound by written confidentiality obligations at least as protective as those in this Section; and

d) promptly notify the Disclosing Party of any unauthorised access, use, or disclosure.

11.3 Permitted Disclosures

The Receiving Party may disclose Confidential Information if required by law, court order, or regulatory request, provided it:

a) gives the Disclosing Party advance notice (unless legally prohibited); and

b) cooperates to obtain a protective order or other remedy.

11.4 Exclusions

Confidential Information does not include information that the Receiving Party can demonstrate:

a) was already lawfully known to it without restriction;

b) was independently developed without use of the Disclosing Party's information;

c) is or becomes publicly available through no fault of the Receiving Party; or

d) was lawfully received from a third party without breach of confidentiality.

11.5 Return or Destruction

Upon written request—or automatically upon termination under Section 12—the Receiving Party will, at the Disclosing Party's choice, return or securely destroy all Confidential Information (including all copies) and certify completion in writing, except that:

a) one archival copy may be retained solely for legal or compliance purposes and kept confidential; and

b) log entries or backups that are technically impracticable to delete will be protected by continuing confidentiality obligations.

11.6 Duration

These confidentiality obligations survive five (5) years after the latter of:

a) termination of the Service Agreement; or

b) final deletion of Personal Data;

except for trade secrets, which must be kept confidential as long as they remain trade secrets under applicable law.

12 Term and Termination

12.1 Entry into Force

This DPA takes effect on the date of the last signature and remains in force for the full term of the Service Agreement.

12.2 Termination Events

a) **Ordinary termination.** This DPA terminates automatically when the Service Agreement expires or is lawfully terminated by either Party.

b) **Termination for breach.** Either Party may terminate this DPA with immediate effect by written notice if the other Party materially breaches this DPA and fails to remedy the breach within thirty (30) calendar days of receiving a written notice specifying the breach.

c) **Termination required by law.** If continuing the Processing would violate Applicable Law or a binding order of a competent authority, either Party may terminate this DPA immediately upon written notice.

12.3 Effect of Termination

Upon termination of the Service Agreement or this DPA (whichever occurs first):

a) Dentio will cease all Processing of Personal Data except that which is necessary to perform its post-termination obligations.

b) Dentio will delete or return Personal Data in accordance with the export window and hard-delete deadline described in Section 8.

c) Sections that by their nature survive termination—confidentiality (Section 11), liability (Section 10), dispute resolution (Section 13), and data-retention obligations (Section 8)—remain in effect until fulfilled or expired.

12.4 No Automatic Termination Rights

Termination or expiry of this DPA does not by itself entitle either Party to any refund or compensation except as expressly provided in the Service Agreement.

13 Governing Law and Dispute Resolution

13.1 Governing Law

This DPA—together with any non-contractual obligations arising out of or in connection with it—shall be governed by and construed in accordance with the laws of Sweden, without regard to its conflict-of-laws rules.

13.2 Amicable Resolution

The Parties shall first attempt in good faith to settle any dispute, controversy or claim arising under or in connection with this DPA (a "Dispute") through negotiations between their respective executive contacts. Negotiations will be deemed to have failed if no settlement is reached within thirty (30) calendar days after written notice of the Dispute.

13.3 Arbitration

If the Dispute is not resolved under Section 13.2, it shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (SCC) under its Rules for Expedited Arbitrations in force on the date the notice of arbitration is submitted.

a) **Seat (place of arbitration):** Stockholm, Sweden.

b) **Language:** Swedish (documents in English may be accepted).

c) **Effect:** The arbitral award shall be final and binding on the Parties.

13.4 Interim Relief

Nothing in this Section 13 shall prevent either Party from applying to the Stockholm District Court (Stockholms tingsrätt) or other court of competent jurisdiction for interim injunctive relief to prevent irreparable harm.

13.5 Cooperation with Supervisory Authorities

Both Parties agree to cooperate fully, in good faith, with the Swedish Authority for Privacy Protection (IMY) or any other competent supervisory authority in the event of investigations or enquiries relating to the Processing of Personal Data under this DPA.

14 Service Data and Analytics

14.1 Permitted Processing of Service Data

The Controller acknowledges and agrees that Dentio may collect, use, and process Service Data for its own legitimate business purposes, including:

a) accounting, billing, audit, and compliance purposes;

b) providing, improving, developing, and optimising the Services;

c) investigating fraud, security threats, or misuse of the Services;

d) generating anonymised benchmarks and industry insights; and

e) as otherwise permitted by Applicable Law.

14.2 Exclusion from Personal Data Obligations

For the avoidance of doubt, Service Data is not Customer Personal Data and the obligations set out in this DPA regarding Personal Data do not apply to Dentio's processing of Service Data.

14.3 De-identification Standards

Dentio warrants that any de-identification or anonymisation of data used to create Service Data shall be performed using industry-standard techniques and shall be irreversible, such that the resulting data cannot reasonably be used to identify any individual Data Subject.

14.4 No Additional Fees

The Controller acknowledges that no additional fee or remuneration is due for Dentio's processing of Service Data under this Section.

15 Use of Data for Artificial Intelligence and Machine Learning

15.1 Prohibition on AI/ML Training

Dentio shall not use any Personal Data processed on behalf of the Controller for the purpose of training, retraining, fine-tuning, or otherwise developing any artificial intelligence or machine learning models, except as strictly necessary to provide the Services.

15.2 Purpose Limitation

Personal Data shall be processed solely for the purposes of providing, maintaining, securing, and supporting the Services as described in this DPA and Annex 1.

15.3 Anonymised Data for Insights

Dentio may process fully anonymised and aggregated Service Data for statistical reporting, security analysis, or operational insights, provided that such information cannot be used to identify the Controller, its patients, or any natural person.

dentio.

Annex 1 — Detailed Instructions for Processing

The Processing activities described below involve special categories of Personal Data within the meaning of Article 9 GDPR, specifically data concerning health. Patient consultations recorded and transcribed through the Services contain clinical observations, symptoms, treatment discussions, and other health-related information. The Controller is responsible for ensuring an appropriate legal basis exists under both Article 6 and Article 9 GDPR.

#	Processing activity	Purpose (Approved Purpose)	Categories of personal data	Categories of data subjects	Maximum retention (see § 8)
1	**Speech-to-text transcription** of recorded consultations	Convert voice to text for later drafting	Audio stream containing patient voice; incidentally captured identifiers and clinical observations	Patients visiting the Controller's clinic	Raw audio ≤ 24 h
2	**AI draft generation** (summaries, referral templates, journal text, odontogram, periodontal chart)	Supply a structured, editable draft for clinician review	Consultation transcript, metadata (recording time, user ID)	Same as row 1	Draft text 30 days
3	**Copy-paste into EHR** via user interface	Allow clinician to insert verified note into local patient record system	Draft text only (no additional identifiers)	Same as row 1	Not stored by Dentio once pasted
4	**Application & security logging**	Forensic readiness, legal accountability, intrusion detection	Pseudonymised patient reference (hash), user ID, timestamp, IP, event type	Clinic personnel; patients (hashed)	Maximum retention: 400 days
5	**Daily encrypted back-ups**	Disaster-recovery resilience	Encrypted snapshots of DB blobs/files	All of the above	30 days
6	**Service analytics (aggregate)**	Product performance statistics	Fully anonymised counts, durations, error codes (no identifiers)	n/a (anonymous)	Indefinite (anonymised)
7	**BankID authentication**	Identity verification of clinic personnel	Social security numer, name, authentication timestamp	Clinic personnel	During term of agreement

dentio.

Annex 2 — Technical and Organisational Measures (TOMs)

The measures below are implemented and operational unless a "road-map" note is indicated.

1. Governance and Policy

Dentio maintains an ISO 27001-aligned Information Security Management System (ISMS) with annual management review. A security steering group chaired by the CEO/DPO conducts quarterly risk register reviews.

2. Access Control

Dentio implements role-based access control with least-privilege defaults. Staff have zero access to patient text by default.

3. Encryption and Key Management

All data at rest is encrypted using AES-256 with Google-managed encryption keys rotated yearly. All data in transit is protected by TLS 1.2 or higher, with HSTS enabled for 12 months.

4. Data Minimisation and Retention Enforcement

Raw audio is chunked, stored in tmpfs, and purged automatically through overwrites. Thirty-day object-lifecycle rules govern retention. Application logs retained for up to 400 days, depending on log type (infrastructure vs. application). Retention aligned with forensic and security requirements and auto-deleted thereafter.

5. Segregation and Tenant Isolation

Customer data is isolated using Supabase row-level security, schema separation, and user-specific encryption keys.

6. Backup and Disaster Recovery

Daily encrypted snapshots are stored in eu-north-1 with a Recovery Point Objective (RPO) of 24 hours or less. Backups inherit deletion policies when source objects expire, with a 30-day hard limit.

7. Incident Response

Dentio maintains 24 × 7 on-call coverage with documented incident playbooks. Mandatory post-mortems are completed within 10 business days of any incident. The Controller is notified within 24 hours of a confirmed Personal Data Breach (see Section 6).

8. Personnel and Training

Background checks are required for all staff with production access. All personnel complete privacy and security training at hire and annually thereafter, with completion tracked.

9. Physical Security

All AI inference runs in ISO 27001- and SOC 2-certified Google Cloud Platform data centres located in Finland, Netherlands, Germany, France, Poland, and Sweden. Dentio does not operate any on-premise hosting.

Annex 3 — Approved Sub-Processors

Annex 3 — Approved Sub-Processors

Any future Sub-Processor will be added here following the notice & objection procedure in § 4. Last updated: 26 November 2025

Provider	Purpose	Processing Location	Notes / Data Location
Google Cloud (EMEA Ltd.)	Serverless functions, secret management, load balancing, storage, AI models (Vertex AI Gemini 2.5 Pro / Gemini 2.5 Flash / Gemini 2.5 Flashlite), transcription, telemetry	EU	EU regions `europe-north1` (Hamina, Finland) and `europe-north2` (Stockholm, Sweden). No transfers outside the EU. All production infrastructure (APIs, backend services) runs on Google Cloud Run (Serverless).
AWS EMEA SARL	AI inference for structured clinical documentation (Claude 3.5 series).	EU	EU-only processing via AWS EU region `eu-north-1` (Stockholm). Zero retention; no model training. All content encrypted using Dentio-managed keys; data never leaves the EU.
Microsoft Azure	AI-assisted drafting and reasoning (OpenAI GPT models via Azure OpenAI Service).	EU	EU-only (Azure EU regions). Zero retention; no model training; inference only. All content double-encrypted with Dentio-managed keys; no transfers outside the EU.
Supabase Ltd.	Managed PostgreSQL database, authentication	EU according to GDPR	Hosted in eu-north-1 (AWS). Used for structured data (clinic, session, and user management). No storage or file hosting. Draft text automatically deleted after 30 days in accordance with Section 8.2.
GitHub Inc.	Source control, CI/CD via GitHub Actions, Collaborative Code Deployment	EU	EU-hosted repositories and runners. Builds and deploys serverless services to Google Cloud. No patient data stored or processed. SOC 2 Type II certified.
Netlify Inc	Frontend hosting, build automation, CDN Distribution of webapp	EU	EU-hosted build and origin servers. Deployed static frontend assets are distributed via Netlify's EU CDN nodes. No backend logic or patient data is stored or processed. Only

			publicly served application assets and minimal deployment metadata (e.g. commit info, build logs) are handled. SOC 2 Type II certified.
Sentry Inc.	Application performance monitoring, error tracking, and exception logging for Dentio's web and backend services	EU	EU region deployment (sentry.io EU). Non-identifiable diagnostic data such as error messages, stack traces, and performance metrics. No patient data, user content, or audio/text data is transmitted. SOC 2 Type II certified.
Soniox Inc.	Real-time speech recognition and transcription for clinical audio recordings	EU	EU processing only. Audio is processed in real-time streaming and deleted immediately upon transcription completion (zero retention). No transfers outside EEA. ISO 27001 and SOC 2 Type II certified.
Posthog Inc.	Product analytics and feature flagging for platform improvement	EU	PostHog EU Cloud (hosted within EU). Collects anonymised usage metrics only: page views, feature interactions, click events, session duration, browser type. No patient data, clinical content, or transcripts transmitted. SOC 2 Type II certified.
Finansiell ID-Teknik BID AB	*Secure authentication services (BankID)*	EU	Sweden only. BankID is issued and operated exclusively within Sweden. Personnummer and authentication tokens processed at point of login; no data retained by BID beyond the authentication transaction.

Effective Date per the date of signature below

Signatures

For the Controller:

Name: _____

For Dentio AB:

Elias Afrasiabi

dentio.

Title: _____ CEO

Date: _____ Date: _____