Data Processing Agreement

Version: 1.0
Published: June 2026
Effective: Upon electronic acceptance at account registration

---

Parties

This Data Processing Agreement ("DPA") is entered into between:

Controller: The legal entity identified by the company name and business details provided at account registration on app.velvoite.eu ("Customer", "Controller"); and

Processor: Silly Pilot Oy, Business ID 3572343-6, Laidunkuja 5C, Espoo, Finland ("Provider", "Processor").

Acceptance. This DPA is accepted electronically. By checking the "I accept the Data Processing Agreement" checkbox during registration on app.velvoite.eu, the person completing registration confirms that they have authority to bind the Controller to this DPA. The date, time, document version, and IP address of acceptance are recorded by the Processor and constitute binding acceptance of this DPA by the Controller.

This DPA forms part of and is incorporated into the Terms of Service ("ToS") between the parties. In the event of conflict between this DPA and the ToS on matters relating to personal data processing, this DPA prevails.

---

1. Definitions

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

"Personal Data", **"Controller"**, **"Processor"**, **"Processing"**, **"Data Subject"**, **"Personal Data Breach"**, and **"Supervisory Authority"** have the meanings given in Article 4 GDPR.

"Sub-processor" means any third party engaged by the Processor to carry out processing activities in respect of the Controller's Personal Data.

"Services" means the Velvoite regulatory compliance monitoring platform and associated services as described in the ToS.

"TOMs" means the technical and organisational measures set out in Annex II.

"DORA" means Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector.

---

2. Scope and Roles

2.1 This DPA applies to the Processor's Processing of Personal Data on behalf of the Controller in connection with the provision of the Services, as described in Annex I.

2.2 The Controller is the Controller of Personal Data submitted to or generated within the Services in respect of the Controller's authorised users and any Personal Data contained in documents uploaded by the Controller.

2.3 The Processor acts as Processor in respect of such Personal Data. The Processor acts as independent Controller in respect of its own account, billing, and operational data — such processing is governed by the Processor's Data Protection Policy, not this DPA.

2.4 Each party shall comply with its respective obligations under applicable data protection law in connection with Personal Data processed under this DPA.

---

3. Processing Instructions

3.1 The Processor shall process Personal Data only on the documented instructions of the Controller. The ToS and this DPA constitute the Controller's complete instructions as of the date of execution. The Controller may issue further written instructions by email to **legal@velvoite.eu**, provided such instructions are technically feasible and do not require the Processor to act outside the agreed scope of the Services.

3.2 If the Processor is required by Union or Member State law to process Personal Data otherwise than on the Controller's instructions, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such disclosure.

3.3 The Processor shall promptly notify the Controller if, in the Processor's opinion, an instruction infringes the GDPR or applicable data protection law. The Processor is not required to perform manifestly unlawful instructions.

---

4. Confidentiality

4.1 The Processor shall ensure that persons authorised to process Personal Data under this DPA are bound by an obligation of confidentiality with respect to that Personal Data, whether by contract or by statutory duty.

4.2 Access to Personal Data shall be limited to those personnel who need access to provide the Services.

---

5. Security

5.1 The Processor shall implement and maintain the technical and organisational measures set out in Annex II, which the parties agree provide a level of security appropriate to the risks presented by the Processing.

5.2 The Processor may update the TOMs from time to time, provided the updated measures do not materially reduce the level of protection afforded to Personal Data. Material reductions require prior written notice to the Controller of at least 30 days.

5.3 The Processor shall ensure that Sub-processors implement equivalent technical and organisational measures with respect to the Personal Data they process.

---

6. Sub-processors

6.1 The Controller grants general written authorisation for the Processor to engage the Sub-processors listed in Annex III as of the date of this DPA.

6.2 The Processor shall notify the Controller of any intended addition or replacement of a Sub-processor at least **30 days** before the change takes effect, by email to the Controller's registered account email address and by publication on the Processor's legal documentation page at velvoite.eu/legal.

6.3 The Controller may object to a new or replacement Sub-processor on reasonable grounds related to data protection within 14 days of notification. If the parties cannot resolve the objection within a further 14 days, the Controller may terminate the relevant Services on 30 days' written notice without penalty.

6.4 The Processor shall impose on each Sub-processor, by written contract, data protection obligations equivalent to those imposed on the Processor by this DPA. The Processor remains fully liable to the Controller for the performance of Sub-processors' obligations.

---

7. Data Subject Rights

7.1 The Processor shall, insofar as technically feasible, assist the Controller by appropriate technical and organisational measures in fulfilling the Controller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III GDPR (including rights of access, rectification, erasure, restriction, portability, and objection).

7.2 The Processor shall promptly notify the Controller — and in any event within **5 business days** — of any Data Subject request received directly by the Processor that relates to Personal Data processed under this DPA. The Processor shall not respond to such requests on the Controller's behalf without prior written authorisation from the Controller, except to acknowledge receipt.

7.3 The Processor shall make available to the Controller, on request, the information in its systems relating to the Controller's Personal Data that is necessary to respond to a Data Subject request. The Processor may charge a reasonable fee for excessive requests.

---

8. Assistance with Controller Obligations

8.1 The Processor shall assist the Controller in ensuring compliance with the obligations under Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments, and prior consultation), taking into account the nature of the Processing and the information available to the Processor.

8.2 The Processor shall maintain the records necessary to demonstrate its compliance with this DPA and make them available to the Controller on reasonable written request.

---

9. Personal Data Breach Notification

9.1 The Processor shall notify the Controller **without undue delay**, and in any event **within 48 hours** of becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA.

9.2 Breach notification shall be sent to the Controller's registered account email address and shall include, to the extent then known: (a) the nature of the breach, including categories and approximate number of Data Subjects and records affected; (b) the name and contact details of the data protection contact point; (c) likely consequences of the breach; and (d) measures taken or proposed to address the breach. Information may be provided in phases where complete details are not yet available.

9.3 **DORA-specific notification:** Where the Controller is a financial entity subject to Regulation (EU) 2022/2554 (DORA) and the breach constitutes or may constitute a major ICT-related incident within the meaning of Article 3(8) DORA, the Processor shall provide an initial notification to the Controller **within 4 hours** of classifying the incident as major to enable the Controller to fulfil its obligations under DORA Article 19. This initial notification may be brief and shall be followed by a full notification under clause 9.1 as further information becomes available.

9.4 The Processor's notification under this Section does not constitute an admission of fault or liability.

---

10. International Transfers

10.1 The Processor shall not transfer Personal Data outside the European Economic Area ("EEA") except as set out in this Section.

10.2 The Processor transfers Personal Data to the Sub-processors listed in Annex III who are established outside the EEA. Each such transfer is subject to the safeguards set out in Annex III for that Sub-processor, which may include: (a) Standard Contractual Clauses adopted by the European Commission (Decision 2021/914); (b) adequacy decisions of the European Commission; or (c) certification under the EU-US Data Privacy Framework (DPF).

10.3 The Processor warrants that, as at the date of this DPA, it has executed or received Standard Contractual Clauses (or equivalent adequate safeguard) from each Sub-processor listed in Annex III that processes Personal Data outside the EEA.

10.4 The Processor shall notify the Controller promptly if the legal basis for an international transfer is no longer valid, and shall cooperate with the Controller to establish an alternative lawful transfer mechanism.

---

11. Audit and Inspection

11.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and with Article 28 GDPR, and shall allow for and

contribute to audits and inspections conducted by the Controller or a mutually agreed independent third-party auditor.

11.2 Audit requests shall be made in writing with reasonable notice of at least **30 days**, conducted during normal business hours, and shall not unreasonably disrupt the Processor's operations. The Controller shall bear the cost of any audit unless the audit reveals a material breach of this DPA, in which case costs shall be borne by the Processor.

11.3 **Third-party certification:** As an alternative to a Controller-conducted audit, the Processor may satisfy audit requests by providing relevant third-party audit reports or certifications (such as SOC 2 Type II or ISO 27001 certification) where these cover the scope of the audit request. The Controller retains the right to conduct its own audit where third-party certification does not cover the matters in scope.

11.4 **Regulatory access:** Where the Controller is a regulated financial entity and its Supervisory Authority (including the Finnish Financial Supervisory Authority (FIN-FSA) or the German Federal Financial Supervisory Authority (BaFin)) exercises inspection powers that require access to the Processor's premises, systems, or records, the Processor shall cooperate with such access to the extent legally permissible and to the extent necessary for the regulatory inspection.

---

12. Deletion and Return of Data

12.1 Upon termination or expiry of the ToS for any reason, the Processor shall, at the Controller's choice: (a) return to the Controller a copy of all Personal Data processed under this DPA in a structured, commonly used, machine-readable format; or (b) securely delete all Personal Data processed under this DPA.

12.2 The Controller must notify the Processor of its choice under clause 12.1 **within 30 days** of termination. If no election is made within that period, the Processor shall delete the Personal Data in accordance with its Data Retention Schedule.

12.3 The Processor shall certify in writing to the Controller that deletion has been completed, within 30 days of deletion.

12.4 The Processor may retain Personal Data beyond the deletion period to the extent required by Union or Member State law, provided such data is processed only for the purposes of that legal requirement and is protected by appropriate technical measures.

---

13. Liability and Indemnity

13.1 Each party's liability under this DPA is subject to the limitations and exclusions in Section 11 of the ToS.

13.2 Notwithstanding clause 13.1, nothing in this DPA limits either party's liability: (a) to Data Subjects under Article 82 GDPR; (b) for fraud or fraudulent misrepresentation; or (c) for any other liability that cannot be excluded or limited under applicable Finnish law.

13.3 If either party pays compensation to a Data Subject under Article 82 GDPR for damage caused by a breach of this DPA or GDPR, the other party shall, to the extent it is responsible for the damage, indemnify the paying party.

---

14. Term

14.1 This DPA takes effect on the date the Controller accepts the ToS and remains in force for as long as the Processor processes Personal Data on behalf of the Controller.

14.2 This DPA terminates automatically upon termination or expiry of the ToS, subject to the Processor's obligations regarding deletion and return under Section 12, which survive termination.

---

15. Governing Law

15.1 This DPA is governed by the laws of Finland, excluding its conflict of law provisions.

15.2 Any dispute arising from this DPA shall be resolved in accordance with the dispute resolution provisions of the ToS.

---

16. Amendments

16.1 This DPA may be amended by mutual written agreement of the parties.

16.2 If changes to applicable data protection law require amendments to this DPA, the Processor may propose amendments by providing the Controller with 30 days' written notice. If the Controller does not object within that period, the amendments take effect at the end of the notice period. If the Controller objects, the parties shall negotiate in good faith.

Acceptance Record

This DPA is accepted electronically at account registration. No handwritten signatures are required.

How acceptance is recorded. When the Controller's authorised representative completes registration on app.velvoite.eu and checks the "I accept the Data Processing Agreement" checkbox, the Processor records the following in its secure database:

Field	Content
Document type	`dpa`
Document version	Version number of this DPA as displayed at time of registration
Accepted at	UTC timestamp of acceptance
IP address	IP address from which registration was completed
User agent	Browser/client identifier
Authority confirmed	`true` — the registering person confirmed they have authority to bind their company
Company	Company name and ID as registered
Accepted by	Name and email of the person who completed registration

Requesting an acceptance record. The Controller may request a copy of their acceptance record at any time by emailing legal@velvoite.eu.

Enterprise customers. Regulated financial entities that require a countersigned paper DPA for regulatory or procurement purposes may request one by contacting legal@velvoite.eu. The countersigned DPA supersedes this click-through acceptance for that customer.

Annex I — Description of Processing

I.1 Subject Matter

The Processor provides the Controller with access to the Velvoite regulatory compliance monitoring platform, including AI-assisted regulatory document monitoring, obligation extraction, deadline tracking, and gap analysis tools ("Services"), as further described in the ToS.

I.2 Duration of Processing

For the duration of the subscription term under the ToS, and for such additional periods as are necessary for the Processor to perform its obligations upon termination (deletion, return).

I.3 Nature and Purpose of Processing

Nature	Purpose
Storage of search query text	To provide the regulatory search and semantic query functionality of the Services
Storage and retrieval of user account data	To authenticate users and provide personalised access to the Services
Transmission of search query text to AI providers	To enable AI-powered semantic search and regulatory monitoring
Storage of uploaded documents (Gap Mapper)	To perform regulatory gap analysis against the Controller's internal policies and procedures
Transmission of uploaded document content to AI providers	To enable AI-assisted gap analysis and obligation matching
Deletion of personal data on termination	To fulfil the Processor's obligations under this DPA and GDPR

I.4 Types of Personal Data

Category	Examples	Incidental?
User account identifiers	Name, email address, professional title, employer name	No — collected at registration
Search query content	Free-text regulatory queries submitted via web UI, API, or MCP, which may incidentally contain names, company names, or other personal identifiers	Incidental — typically contains regulatory terminology

Category	Examples	Incidental?
Uploaded document content (Gap Mapper)	Text of internal compliance policies, procedures, and frameworks, which may contain names, job titles, signatures, and contact details of the Controller's personnel	Incidental — content determined by the Controller

I.5 Categories of Data Subjects

- The Controller's employees, contractors, and authorised users who access the Services.
- Natural persons incidentally mentioned in search queries submitted to the Services.
- Natural persons incidentally mentioned in documents uploaded by the Controller to the Gap Mapper feature.

I.6 Special Categories of Data

The parties do not anticipate that the Controller will submit special category data (as defined in GDPR Article 9) to the Services. The Controller warrants that it will not submit special category data without prior written agreement with the Processor.

Annex II — Technical and Organisational Measures

The Processor implements the following technical and organisational measures with respect to Personal Data processed under this DPA.

Encryption

- Data in transit: TLS 1.3
- Data at rest: AES-256 (Google Cloud SQL, Memorystore Redis)
- API keys: SHA-256 hashed, never stored in plaintext

Access Control

- Role-based access control (RBAC) with principle of least privilege
- Multi-factor authentication available for administrative access
- API key authentication with per-customer isolation
- JWT-based session management with expiry

Infrastructure

- All Customer Personal Data stored in Google Cloud Platform, europe-north1 region (Finland), within the EEA
- Separate database-level tenant isolation
- Automated daily backups with point-in-time recovery (Cloud SQL)
- Redis caching layer (GCP Memorystore, europe-north1)

Sub-processor Controls

- Sub-processors are engaged under written contracts imposing equivalent data protection obligations
- All US-based Sub-processors operate under Standard Contractual Clauses (Commission Decision 2021/914) and/or EU-US Data Privacy Framework certification

Organisational Measures

- Data protection training for all personnel with access to Personal Data
- Confidentiality obligations for all personnel
- Written incident response procedure with defined escalation path
- Data breach notification process as set out in Section 9 of this DPA
- Annual DPIA review (next review: May 2027)
- Vendor due diligence on Sub-processors before engagement

Monitoring and Logging

- Security logging via Google Cloud Logging (europe-north1)
- AI processing logs retained for 6 months per EU AI Act Article 26(6)
- Automated anomaly detection

AI Processing Safeguards

- AI-generated outputs are labelled as AI-generated throughout the Services
- Regulatory obligation text is presented in verbatim form alongside AI summaries
- No automated decisions with legal effect are made without human review
- Customer data is not used to train AI models (contractually prohibited in all Sub-processor agreements)

Annex III — Approved Sub-processors

The following Sub-processors are authorised as of the date of this DPA to process Personal Data submitted to or generated by the Controller's use of the Services.

Sub-processor	Entity	Location	Data Processed	Transfer Safeguard
Google Cloud Platform (GCP)	Google LLC	EU (europe-north1, Finland)	All Customer Personal Data — stored and served within the EEA	EEA — no transfer; DPA in place
Google Gemini API	Google LLC	United States	Search query text; uploaded document content (where transmitted for AI processing)	SCCs (Commission Decision 2021/914, Module 2: C→P); EU-US DPF certified
Anthropic Claude API	Anthropic PBC	United States	Search query text submitted via MCP integration	SCCs (Commission Decision

Sub-processor	Entity	Location	Data Processed	Transfer Safeguard
				2021/914, Module 2: C→P)

Notes:

1. Stripe (payment processing) and Resend (email delivery) process data for which the Processor is the independent Controller (billing data and outbound communications). These are not Sub-processors under this DPA.
2. Plausible Analytics processes only anonymised, aggregated usage metrics with no personal data — it is not a Sub-processor under this DPA.
3. Sub-processor changes are notified per Section 6.2 of this DPA.

Annex IV — DORA ICT Third-Party Register Information

Complete where the Controller is a financial entity subject to DORA.

The Processor provides the following information to assist DORA-regulated Controllers in maintaining their ICT third-party service register per Article 28(3) DORA:

Field	Value
ICT third-party service provider name	Silly Pilot Oy
Business ID	3572343-6
Country of establishment	Finland
LEI code	Not yet obtained
Service description	AI-powered regulatory compliance monitoring platform (SaaS)
Service category	Software as a Service — regulatory intelligence and compliance management
Criticality / importance	To be assessed by Controller per DORA Article 28(2)
Data processed	See Annex I
Sub-ICT providers	Google Cloud Platform (EU), Google Gemini API (US), Anthropic Claude API (US)
Jurisdiction of data storage	European Economic Area (GCP europe-north1, Finland)
Incident notification SLA	4 hours (initial, upon major incident classification) per Section 9.3
Audit rights	Yes — per Section 11 of this DPA
Termination provisions	Section 9 of the ToS; data deletion within 30 days per Section 12 of this DPA