Version 1.0 -- 18 May 2026

Data Processing Agreement

Between MindtheGap Sarl (Processor) and the VeraCita customer (Controller). Governs processing of personal data in connection with the VeraCita citation-verification service.

[LAWYER REVIEW REQUIRED -- DPA DRAFT 2026-05-21]

This DPA reflects the intent of VeraCita's data-processing obligations and is modelled on GDPR Article 28 and Swiss nDSG/FADP requirements. Cohort users may execute as-is pending formal review. Institutional customers (law firms, universities, regulated entities) should request a counter-signed version after lawyer review. Last internal review: Andy Christen, founder, MindtheGap Sarl, 18 May 2026. Send review queries to legal@veracita.ai.

This document: View online (HTML) Download PDF

Request counter-signed copy

TABLE OF CONTENTS

1. Parties and Definitions

1.1 The Parties

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

Role	Identity	Details
Controller	The VeraCita customer (individual or entity) who has accepted the VeraCita Terms of Service	As identified in the VeraCita account registration
Processor	MindtheGap Sarl	CHE-398.557.351 (Geneva Commercial Register) Registered address: Geneva, Switzerland Legal representative: Andy Christen, founder Data contact: legal@veracita.ai

Controller and Processor are each referred to as a "Party" and collectively as the "Parties."

1.2 Definitions

- **"Agreement"** means the VeraCita Terms of Service between the Parties, of which this DPA forms an integral part.
- **"Controller"** means the natural or legal person who determines the purposes and means of the processing of personal data, within the meaning of GDPR Art. 4(7) and nDSG Art. 5(j).

- **"Processor"** means a natural or legal person which processes personal data on behalf of the Controller, within the meaning of GDPR Art. 4(8) and nDSG Art. 5(k).
- **"Personal Data"** means any information relating to an identified or identifiable natural person, within the meaning of GDPR Art. 4(1) and nDSG Art. 5(a).
- **"Processing"** has the meaning given in GDPR Art. 4(2) and nDSG Art. 5(d).
- **"Data Subject"** means an identified or identifiable natural person to whom Personal Data relates.
- **"Sub-Processor"** means any Processor engaged by MindtheGap Sarl to process Personal Data on behalf of the Controller.
- **"Services"** means the VeraCita citation-verification SaaS platform and associated features provided under the Agreement.
- **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- **"nDSG"** means the Swiss Federal Act on Data Protection (Bundesgesetz uber den Datenschutz) in force from 1 September 2023, including implementing ordinances.
- **"EEA"** means the European Economic Area.
- **"SCCs"** means Standard Contractual Clauses adopted by the European Commission pursuant to GDPR Art. 46(2)(c).

1.3 Precedence

In the event of a conflict between this DPA and the Agreement, the terms of this DPA shall prevail with respect to the processing of Personal Data. In the event of a conflict between this DPA and applicable data protection law, the applicable law prevails.

2. Subject Matter

This DPA governs the processing of Personal Data by MindtheGap Sarl (Processor) on behalf of the Controller in connection with the provision of the VeraCita citation-verification service ("Services").

The Services enable the Controller to upload or reference documents containing cited claims, which the platform then verifies against referenced or retrieved sources using AI-

assisted analysis. The Processor processes Personal Data strictly as necessary to perform the Services described in the Agreement and this DPA.

> **Architectural note:** VeraCita is architected to minimise Personal Data exposure. In Zero-Knowledge mode, source documents travel from the Controller's browser directly to the AI inference layer without transiting Processor servers. In Standard mode, source text transits Processor memory only (~10 seconds) and is never written to persistent storage. See Privacy Architecture for full technical detail.

3. Nature and Purpose of Processing

3.1 Nature

The Processor will carry out the following processing operations on Personal Data:

- Collection and temporary storage of account registration data (name, email, organisation);
- Storage of verification results (claim text, verdict labels, source references, confidence scores) associated with the Controller's account;
- Processing of billing and usage data (token counts, claim counts, credit balance, payment identifiers);
- Transmission of document content (which may contain Personal Data) to AI inference sub-processors solely for the purpose of citation verification;
- Generation and delivery of audit reports and exports as requested by the Controller.

3.2 Purpose

Processing is carried out for the following purposes:

- Providing the citation-verification Services in accordance with the Agreement;
- Account management, authentication, and access control;
- Billing and credit management;

- Service improvement and security monitoring (using anonymised, aggregated data only -- no individual source content);
- Compliance with applicable legal obligations.

The Processor shall not process Personal Data for any purpose other than those specified above, unless instructed in writing by the Controller or required by applicable law.

4. Personal Data and Data Subjects

4.1 Categories of Personal Data

Category	Examples	Processing basis
Account identity data	Name, email address, organisation name, account ID	Contract performance (GDPR Art. 6(1)(b)); nDSG Art. 31(2)(a)
Usage and billing data	Credit balance, token counts, claim counts, subscription tier, payment reference (not card data)	Contract performance; legitimate interests (billing integrity)
Verification session metadata	Timestamps, document type, claim count, mode selected (Standard / ZK)	Contract performance; legitimate interests (service delivery)
Verification results	Claim text, verdict label, source citation, confidence score -- as submitted by the Controller	Contract performance; Controller's instructions
Document content (transient)	Uploaded source documents or web-fetched source URLs that may contain Personal Data about third parties	Contract performance; strictly ephemeral (Standard mode only -- see Section 2)

No special category data (GDPR Art. 9) is intentionally processed as part of the Services. The Controller is responsible for ensuring that documents submitted do not require

special-category processing unless the Controller obtains the necessary legal basis independently.

4.2 Categories of Data Subjects

- **Controllers and authorised users:** individuals who create or use a VeraCita account on behalf of the Controller;
- **Third parties referenced in submitted documents:** authors, cited sources, or other natural persons named in documents the Controller submits for verification (transient processing only);
- **Third parties referenced in verification results:** natural persons identified in claim text or source text as stored in the Controller's verification history.

5. Duration of Processing

1. **Active subscription:** The Processor shall process Personal Data for as long as the Controller maintains an active account or subscription under the Agreement.
2. **Source content:** Document content transmitted in Standard mode is held in Processor memory during the verification call only (typically under 10 seconds) and is never written to persistent storage. Source content is never retained by the Processor beyond the active verification call.
3. **Verification results:** Claim text, verdicts, and source citations associated with a session are retained for **30 days** from the date of the verification session, then permanently deleted, unless the Controller exports them before deletion.
4. **Session data:** Per the VeraCita Privacy Policy, individual session identifiers are retained for **7 days** then deleted.
5. **Billing metadata:** Token counts, credit debits, and payment references are retained for **24 months** for billing dispute resolution, then deleted.
6. **Account data:** Upon termination of the Agreement or deletion of the Controller's account, the Processor shall, at the Controller's election (stated in the termination

notice), either delete or return all Personal Data within **30 days** of the effective termination date, subject to Section 13 below.

7. **Legal holds:** The Processor may retain Personal Data beyond the above periods where required by applicable Swiss or EU law, for the duration and to the extent required by that law only.

6. Processor Obligations

1. **Documented instructions:** The Processor shall process Personal Data only on documented instructions from the Controller, unless processing is required by applicable law. The Agreement and this DPA constitute the Controller's initial set of instructions.

2. **Confidentiality:** The Processor shall ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. **Security:** The Processor shall implement and maintain the technical and organisational measures described in Section 9 of this DPA.

4. **Sub-processors:** The Processor shall only engage sub-processors in accordance with Section 8 of this DPA and shall impose the same data protection obligations on any sub-processor.

5. **Data Subject rights:** The Processor shall assist the Controller in fulfilling obligations to respond to requests for exercising the Data Subject's rights under GDPR Chapter III and nDSG Art. 25-27 within applicable timeframes.

6. **Controller assistance:** The Processor shall assist the Controller in ensuring compliance with its obligations under GDPR Art. 32-36 (security, breach notification, DPIA, prior consultation), taking into account the nature of processing and information available to the Processor.

7. **Breach notification:** The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data breach, and in any event within **72 hours** of the Processor's own discovery of the breach, in accordance with Section 10 of this DPA.

8. **Deletion / return:** The Processor shall, at the choice of the Controller, delete or return all Personal Data on termination of the Agreement in accordance with Section 13, unless retention is required by applicable law.

9. **Audit cooperation:** The Processor shall make available to the Controller all information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits in accordance with Section 12.

10. **No onward transfer:** The Processor shall not transfer Personal Data to a third country or international organisation except as expressly permitted under Section 11 and applicable data protection law.

7. Controller Obligations

1. **Legal basis:** The Controller warrants that it has an appropriate legal basis for submitting Personal Data to the Services and that such submission complies with applicable data protection law.

2. **Special categories:** The Controller shall not submit special- category personal data (GDPR Art. 9) or criminal records data (GDPR Art. 10) to the Services without first notifying the Processor in writing and obtaining the Processor's written acceptance.

3. **Data Subject notices:** The Controller is responsible for providing Data Subjects with appropriate privacy notices and obtaining consent or other legal bases for processing, where required.

4. **Instructions:** The Controller is responsible for the legality of its processing instructions. The Controller shall provide lawful instructions only and shall

immediately inform the Processor if, in its opinion, an instruction infringes applicable data protection law.

5. **Data minimisation:** The Controller is responsible for ensuring that only the minimum necessary Personal Data is submitted to the Services.

8. Sub-Processors

8.1 Authorised Sub-Processors

The Controller hereby provides general written authorisation to the Processor to engage the following sub-processors. The Processor shall impose data protection obligations equivalent to those in this DPA on each sub-processor.

Sub-Processor	Purpose	Region	Personal data processed
Amazon Web Services, Inc. (AWS) ***Bedrock, Aurora, Lambda, CloudWatch, S3, API Gateway, Cognito***	AI inference, database, serverless compute, monitoring, identity	AWS eu-central-2 (Zurich, Switzerland)	Account data, verification results, billing records, session metadata, source content (transient in Lambda memory -- Standard mode only)
Anthropic PBC ***via AWS Bedrock***	Large language model inference for claim and source analysis	AWS eu-central-2 (Zurich, Switzerland)	Source text passages and claim text during verification calls; ephemeral prompt cache (max 5 min, account-scoped, no training use)

Sub-Processor	Purpose	Region	Personal data processed
Resend, Inc. ***Transactional email***	Account-related transactional emails (receipts, alerts, verification summaries)	US (EU data subject emails processed under SCCs)	Email address, account name, email content for transactional notifications
Stripe, Inc. ***Payment processing***	Payment processing and billing management	EU / US (SCCs in place)	Payment details (card data held by Stripe only, never by Processor), billing address, transaction records
Infomaniak Network SA ***Static website hosting***	Static website file hosting (veracita.ai marketing site)	Geneva, Switzerland	No Personal Data -- static HTML/CSS/JS files only; no user data transits to Infomaniak

> **Note on Anthropic via Bedrock:** Anthropic models are accessed exclusively through AWS Bedrock in the eu-central-2 (Zurich) region. AWS's enterprise agreement with Anthropic covers data residency within the selected region. Customer data is not used to train Anthropic models. Anthropic never receives data directly from the Processor or Controller.

8.2 Sub-Processor Changes

1. The Processor shall provide **30 days advance written notice** to the Controller before adding or replacing any sub-processor that processes Personal Data. Notice will be given by email to the address on the Controller's VeraCita account and/or by update to this DPA page at veracita.ai/dpa.html.

2. The Controller may object to a new sub-processor on reasonable data-protection grounds by written notice to legal@veracita.ai within 14 days of the notification. If the Parties cannot resolve the objection within a further 30 days, the Controller may terminate the Agreement on written notice without penalty.

9. Technical and Organisational Measures (TOMs)

The Processor has implemented and maintains the following technical and organisational measures to ensure a level of security appropriate to the risk of the processing, in accordance with GDPR Art. 32 and nDSG Art. 8.

9.1 Encryption in Transit

- All communications between users and the Processor's infrastructure are encrypted using TLS 1.3.
- AWS Certificate Manager with automatic certificate renewal is used for all API endpoints.
- API calls to AWS Bedrock are signed using AWS Signature Version 4 (SigV4).
- Zero-Knowledge mode uses short-lived, session-scoped SigV4 credentials (15-minute lifetime) issued to the Controller's browser for direct Bedrock calls.

9.2 Encryption at Rest

- Aurora PostgreSQL database is encrypted at rest using AWS KMS (AES-256) with Processor-managed keys in eu-central-2.
- Documents uploaded by users in Zero-Knowledge mode are stored in the user's browser IndexedDB only; the Processor holds no decryption keys for user content.
- Source documents in Standard mode are processed in Lambda memory and never written to any persistent storage.

9.3 Access Controls

- Row-Level Security (RLS) enforced at the database layer: each Controller's data is isolated by account ID; no query can return another account's data.
- Principle of least privilege applied to all Lambda execution roles and IAM policies.
- Administrative access to production systems is restricted to the founder and requires MFA.
- No employee has routine, standing access to source content or in-memory verification data.

9.4 Data Minimisation and Retention Enforcement

- Source content is never persisted by the Processor in any form.
- Verification results are subject to automated deletion after 30 days (see Section 5).
- Session tokens are invalidated after 7 days.
- Billing metadata is the only long-retention data category (24 months).

9.5 Pseudonymisation and Anonymisation

- Usage statistics used for service improvement are aggregated and anonymised before analysis; no source content is included.
- Internal monitoring dashboards display token and claim counts only -- not source text.

9.6 Availability, Resilience, and Recovery

- AWS Aurora Serverless v2 provides automated failover and point-in-time recovery.
- Lambda functions are deployed across multiple Availability Zones within eu-central-2.
- CloudWatch alarms are configured for latency, error rate, and availability.
- Incident response procedures are documented and tested by the Processor.

9.7 Hybrid Zero-Knowledge Option

- Enterprise Controllers may request Strict Zero-Knowledge workspace mode, in which all source processing is carried out exclusively within the Controller's browser and no source bytes transit Processor infrastructure.
- In this mode, the Processor's TOMs for source content are irrelevant: the Processor never receives the content.

9.8 Sub-Processor Security

- AWS eu-central-2 is certified to ISO/IEC 27001, 27017, 27018; SOC 1/2/3; and BSI C5. Certificates are available via AWS Artifact on request.
- Stripe maintains PCI DSS Level 1 compliance for payment data.

The Processor may update these measures over time where an update improves the overall level of security. The Processor will notify the Controller of any material reduction in

security measures.

10. Data Breach Notification

1. **Notification timeline:** The Processor shall notify the Controller without undue delay and, where feasible, **within 72 hours** of the Processor becoming aware of a Personal Data breach affecting Personal Data processed on behalf of the Controller.

2. **Notification content:** The notification shall include, to the extent available at the time: (a) a description of the nature of the breach, including the categories and approximate number of Data Subjects and records affected; (b) the name and contact details of the Processor's data protection contact; (c) the likely consequences of the breach; (d) the measures taken or proposed to address the breach.

3. **Contact:** Breach notifications shall be sent to the Controller at the email address on the Controller's VeraCita account. The Processor's data protection contact for breach reporting is legal@veracita.ai.

4. **Controller's regulatory obligations:** The Controller is responsible for assessing whether the breach triggers a notification obligation to the competent supervisory authority (e.g., the FDPIC under nDSG, or the relevant EU supervisory authority under GDPR Art. 33) and for making any such notification.

5. **Cooperation:** The Processor shall cooperate with the Controller in investigating the breach and shall provide reasonable assistance to the Controller in preparing any required regulatory notifications.

11. International Transfers

1. **Primary infrastructure:** All primary processing occurs in Switzerland, on AWS eu-central-2 (Zurich). Switzerland has an adequacy decision under GDPR (European Commission Decision C(2000)2304) confirming an adequate level of protection for

transfers from the EU/EEA to Switzerland. Transfers between the EU/EEA and AWS eu-central-2 do not require additional transfer mechanisms.

2. **Resend (transactional email):** Resend is incorporated in the United States. The Processor relies on Standard Contractual Clauses (SCCs, EU Commission Implementing Decision (EU) 2021/914) for transfers of EU/EEA Personal Data to Resend. Resend is also a GDPR-compliant processor and has executed a DPA with the Processor.

3. **Stripe (payment processing):** Stripe processes payment data under its own DPA with Controllers and is certified under the EU-U.S. Data Privacy Framework. The Processor's engagement of Stripe is limited to billing orchestration; payment card data is processed by Stripe directly under Stripe's own privacy and security obligations.

4. **No other third-country transfers:** The Processor does not transfer Personal Data to any other third country or international organisation without the prior written consent of the Controller.

12. Audit Rights

1. **Annual self-attestation:** The Processor shall, upon written request, provide the Controller with a written self-attestation confirming compliance with this DPA, once per calendar year, at no charge to the Controller.

2. **On-request audit:** The Controller may request a more detailed audit or inspection of the Processor's data processing activities. Such an audit: (a) requires at least 30 days written notice to the Processor; (b) shall be conducted by the Controller or a mutually agreed qualified independent auditor at the Controller's cost; (c) shall not unreasonably disrupt the Processor's operations; (d) shall be limited to information directly relevant to the Controller's Personal Data and the Processor's compliance with this DPA; (e) shall be subject to appropriate confidentiality obligations.

3. **AWS infrastructure audits:** Audits of AWS infrastructure are satisfied by the third-party certifications held by AWS (ISO/IEC 27001, SOC 2 Type II, etc.), available via AWS

Artifact. The Controller may request access to relevant AWS Artifact reports through the Processor.

4. **Frequency:** Unless there is a documented breach or regulatory requirement, audit requests are limited to one per calendar year.

13. Deletion and Return at End of Contract

1. **Controller's election:** At any time after the termination or expiry of the Agreement, the Controller may, by written notice to legal@veracita.ai, elect to: (a) receive a machine-readable export of all Personal Data processed on the Controller's behalf (JSON or CSV format); or (b) have all such Personal Data permanently deleted by the Processor.

2. **Deadline:** The Processor shall complete the return or deletion within **30 days** of receiving the Controller's written election.

3. **Confirmation:** The Processor shall provide written confirmation to the Controller once deletion or return is complete.

4. **Legal retention exception:** The Processor may retain Personal Data beyond the above deadline only to the extent required by applicable Swiss or EU law (e.g., accounting records under Swiss Code of Obligations). The Processor shall inform the Controller of any such retention and shall delete the data as soon as the legal retention obligation expires.

5. **Sub-processors:** The Processor shall ensure that sub-processors also delete or return the Controller's Personal Data within the same 30-day window, except where the sub-processor is subject to its own independent legal retention obligation.

14. Liability

1. **Standard cap:** Each Party's aggregate liability to the other under or in connection with this DPA, whether arising in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total fees paid or payable by the Controller to the Processor in the **12 months preceding the event giving rise to the claim**.

2. **Exclusions from cap:** The cap in Clause 14.1 shall not apply to liability arising from: (a) death or personal injury caused by negligence; (b) fraud or fraudulent misrepresentation; (c) a Party's liability to indemnify the other against third-party regulatory fines imposed as a direct result of that Party's breach of applicable data protection law; or (d) any other liability that cannot be limited or excluded by applicable law.

3. **Mutual indemnity:** Each Party shall indemnify and hold harmless the other Party against any fines, penalties, or third-party claims arising from that Party's breach of its obligations under this DPA or applicable data protection law.

4. **Relationship to Agreement:** The liability provisions of this DPA operate alongside, and do not replace, the general limitation of liability provisions in the Agreement, except where expressly stated.

15. Governing Law and Jurisdiction

1. **Governing law:** This DPA is governed by and construed in accordance with the laws of **Switzerland**, without regard to conflicts of law provisions.

2. **Jurisdiction:** Any dispute arising out of or in connection with this DPA that cannot be resolved by good-faith negotiation shall be subject to the exclusive jurisdiction of the courts of **Geneva, Switzerland**.

3. **GDPR compliance:** Where the Controller is established in the EEA, or processes Personal Data of EEA Data Subjects, this DPA shall also be interpreted in a manner consistent with GDPR obligations, as supplemented by any applicable SCCs referenced in Section 11.

4. **nDSG compliance:** This DPA satisfies the requirements for a written agreement between Controller and Processor under the Swiss Federal Act on Data Protection (nDSG) in force from 1 September 2023.

16. Execution

This DPA is incorporated by reference into the VeraCita Terms of Service. By accepting the Terms of Service (including via a click-through acceptance, account creation, or electronic signature), the Controller agrees to be bound by the terms of this DPA.

Institutional customers who require a wet-ink or countersigned version of this DPA may request one by contacting legal@veracita.ai. The countersigned version will reflect the same terms as published here, unless the Parties agree to customer-specific amendments.

FOR THE PROCESSOR

MindtheGap Sarl

CHE-398.557.351
Geneva, Switzerland
Represented by: Andy Christen, founder
Date of publication: 18 May 2026

Signature on countersigned version:

_____

FOR THE CONTROLLER

Customer (as identified in VeraCita account)

Accepted electronically via Terms of Service acceptance.
For a countersigned paper copy, contact: legal@veracita.ai

Signature on countersigned version:

_____

Version history: v1.0 published 18 May 2026. Changes to this DPA will be notified to Controllers at their registered email address and published at veracita.ai/dpa.html with a

new version date. Sub-processor changes are subject to the 30-day notice provision in Section 8.2.