Data Processing AgreementData Processing Agreement

Data Processing Agreement

Last updated: July 2026

This Data Processing Agreement ("Agreement" or "DPA") forms an integral part of the main agreement between Abra B.V., a company incorporated under the laws of the Netherlands with its principal office in Utrecht ("Processor" or "Abra"), and the customer that has entered into that agreement ("Controller").

*Together referred to as "**Parties**".*

Summary

At Abra, we take privacy and data protection seriously. This Data Processing Agreement (DPA) describes how we handle personal data when providing our software and services to customers. It explains which data we process, how we protect it, and the commitments we make under the General Data Protection Regulation (GDPR).

Abra acts as the **Processor** and our customers act as **Controllers**. We only process data on behalf of our customers and always within the European Union, unless otherwise agreed separately.

0. Definitions

1. **Main Agreement** – the primary commercial or service agreement between Abra B.V. ("Abra") and the customer, under which Abra provides its products and services. This DPA forms an integral part of that Main Agreement.

2. **Controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, as defined in Article 4(7) GDPR.

3. **Processor** – Abra B.V., which processes Personal Data on behalf of the Controller, as defined in Article 4(8) GDPR.

4. **Personal Data** – any information relating to an identified or identifiable natural person ("Data Subject"), as defined in Article 4(1) GDPR.

5. **Processing / Processed** – any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, erasure or destruction, as defined in Article 4(2) GDPR.

6. **Data Subject** – an identified or identifiable natural person whose Personal Data is Processed.

7. **Sub-Processor** – any third party engaged by Abra for carrying out specific Processing activities on behalf of the Controller.

8. **Personal Data Breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, as defined in Article 4(12) GDPR.

9. **Technical and Organisational Measures (TOMs)** – the measures implemented by Abra to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

10. **Supervisory Authority** – an independent public authority established under Article 51 GDPR (such as the Autoriteit Persoonsgegevens in the Netherlands).

1. Subject and Roles

1. Abra B.V. ("**Processor**") processes Personal Data on behalf of the customer ("**Controller**").

2. The Controller determines the purposes and means of the processing.

3. This Agreement applies to all processing activities related to Abra's services, including but not limited to **Abra Desktop, Abra SDK, Abra Dashboard, Abra Documentation**, and **Abra Academy**.

2. Duration and Nature of Processing

1. Abra will process Personal Data for the term of the Main Agreement and solely for the purpose of providing, maintaining, and improving its services — including account management, authentication, testing, reporting, payments, and customer support.

2. Abra will process Personal Data only on documented instructions from the Controller, unless otherwise required by law. In that case, Abra shall inform the Controller prior to

such processing unless prohibited by law.

3. If Abra reasonably believes that an instruction from the Controller infringes the GDPR or other applicable Union or Member State data protection provisions, Abra shall immediately inform the controller thereof and may suspend performance of that instruction pending clarification.

3. Categories of Data and Data Subjects

1. **Categories of Personal Data:**
    - Name and surname
    - Email address
    - Organization name
    - IP address
    - Test data (e.g., screenshots, test logs, device information, OS version)
    - Crash reports
    - Product usage and logging data
2. **Categories of Data Subjects:** Employees or other representatives of the Controller.
3. Abra does not process or deliver any special categories of personal data as defined under Article 9 of the GDPR.

4. Confidentiality

Abra ensures that any person acting under its authority who has access to Personal Data is bound by confidentiality obligations and processes such data only as instructed by the Controller.

5. Security Measures

Abra implements technical and organizational measures appropriate to the risk, including:

- Main data storage within the **EU region** (primary: London West; backups in the Netherlands and Germany). Abra Academy data is stored outside the EU.
- Encryption of data in rest + transit (TLS 1.2+)

- Regular backups (retention: **14 days**)
- “Soft delete” mechanism with full deletion upon request

Further details are listed in **Annex 1**.

6. Sub-Processors

1. Abra may engage sub-processors for specific services.
2. Sub-processors are bound by written contracts ensuring data protection obligations equivalent to this DPA.
3. Abra applies a commercially reasonable selection process by which it evaluates the security, privacy, and confidentiality practices of proposed sub-processors that will or may have access to or process Customer Data.
4. Abra remains responsible for their actions.
5. The Controller authorizes the use of the sub-processors listed at our sub-processers page. Abra will maintain an up-to-date list of sub-processors on its website. The Controller may choose to receive notifications of any intended additions or replacements by subscribing to the notification service. If subscribed, the Controller will be notified at least 30 days in advance and may object on reasonable data-protection grounds.
6. The sub-processor list is maintained by Abra as a separate, living document at Abra's sub-processors page and is incorporated into this Agreement by reference. Updates to that list in accordance with this Section 6 do not require an amendment to this DPA.

7. Assistance to Controller

Abra will, as far as possible, assist the Controller in fulfilling obligations under GDPR, including:

- responding to data-subject requests (access, rectification, erasure, etc.),
- conducting data protection impact assessments (DPIAs), and
- consulting with supervisory authorities where required.

Where such assistance requires a material investment of time or resources beyond Abra's standard support services, Abra may charge the Controller reasonable, pre-agreed fees for that assistance.

8. Personal Data Breaches

1. Abra shall notify the Controller of a personal-data breach **without undue delay** and in any event within **48 hours** after becoming aware of it.
2. The notification shall include:
    - a description of the breach,
    - its likely consequences, and
    - the measures taken or proposed to mitigate its effects.
3. Abra will assist the Controller in meeting any legal obligations arising from such a breach.

9. Audits and Compliance

1. Abra will provide all necessary information to demonstrate compliance with this DPA.
2. The Controller may conduct one audit per year with **14 days'** notice, at its own expense, and without disrupting normal business operations.
3. If material non-compliance with this DPA is identified as a result of an audit, Abra shall promptly implement corrective measures. The reasonable costs of any re-audit necessary to verify that such non-compliance has been remedied shall be borne by Abra.
4. At the Controller's request, Abra will make available its current ISO/IEC 270001 certificate (once obtained), Statement of Applicability, and independent penetration test summary. The parties agree that provision of these materials may satisfy the audit right in section 9.2 in whole or in part, in lieu of an on-site audit.
5. Abra maintains records of processing activities carried out on behalf of the Controller, in accordance with Article 30(2) GDPR, and will make these available to the Controller upon reasonable request.

10. Return and Deletion of Data

1. Upon termination of the Main Agreement, the Controller may request deletion or return of all Personal Data.
2. Upon termination of the Main Agreement, the Controller may instruct Abra to either delete or return all Personal Data. Abra shall delete any remaining copies unless Union

or Member State law requires continued storage.

3. Abra shall confirm deletion in writing upon request.

11. International Data Transfers

1. Abra does not host or maintain Personal Data on its own servers. All Personal Data is stored and processed by Abra's authorized sub-processors acting on Abra's behalf.

2. For all Abra Ecosystem products — including **Abra Desktop**, **Abra Dashboard**, and **Abra Documentation** — Personal Data is stored and processed **exclusively within the European Union**. Abra ensures that all sub-processors engaged for these services maintain data centers within the EU/EEA.

3. The **Abra Academy** platform is operated through the service provider **Thinkific**, which stores and processes Personal Data in the **United States**.
   Abra and its sub-processor have implemented the **European Commission's Standard Contractual Clauses (SCCs)** and additional safeguards to ensure an adequate level of data protection in accordance with **Chapter V of the GDPR**.

4. Abra monitors its sub-processors' compliance with these safeguards at least once per year and ensures that any future data transfers outside the EU/EEA will only occur under valid legal mechanisms providing an equivalent level of protection to that required under the GDPR.

5. The additional safeguards referred to in Section 11.3 include, at a minimum, encryption of Personal Data in transit and at rest, contractual confidentiality and access restriction, and security certification (SOC2 or ISO27001) of the sub-processor. Abra has assessed, by way of a transfer impact assessment, that these measures provide a level of protection essentially equivalent to that guaranteed under the GDPR, and will provide a summary of that assessment to the Controller upon request.

12. Liability

1. Each Party is liable for damages resulting from its own breach of this DPA or applicable data-protection law.

2. Abra's total liability under this DPA is limited to the annual fees paid under the Main Agreement, except in cases of gross negligence or wilful misconduct.

3. Nothing in this DPA limits liability where such limitation is not permitted by law.

4. For the avoidance of doubt, the limitation in Section 12.2 applies only to claims

between the Parties under this DPA, and does not limit or affect any administrative fine imposed by a Supervisory Authority, or any claim brought by a Data Subject, against either Party.

13. Governing Law and Jurisdiction

This DPA is governed by **Dutch law**. Disputes shall be submitted to the **competent court of Oost-Brabant, the Netherlands**.

14. Contact persons

For matters relating to this DPA, the Controller may contact Abra via the following points of contact:

- Security Officer / Data Protection Contact - mike@abra.ai
- Privacy Officer / Incident Response Contact - paul@abra.ai

Annex 1 – Technical and Organizational Security Measures

Abra maintains a security program that includes:

- Encryption of data in rest + transit (TLS 1.2+)
- Secure development practices and vulnerability management
- Logging and continuous monitoring of access
- Back-up management (14-day retention, EU locations only)
- (Soft) Data deletion
- Employee confidentiality agreements and security awareness training
- Security, Data protection and Privacy monthly on agenda / periodically awareness training
- Incident-response and breach-notification protocols
- Periodic review and testing of controls
- Access control based on the principle of least privilege, with role-based permissions and multi-factor authentication for administrative access
- Independent penetration testing conducted at least annually starting Q1 2026, with material findings remediated on a risk-based timeline

- Business continuity and disaster recovery procedures, tested periodically, in addition to routine backups
- A dedicated security contact point for reporting suspected vulnerabilities or incidents

Change Log

Date	Description
October 2025	Added IP address as personal data; clarified crash-report processing; specified 14-day backup retention; expanded sub-processor list; added breach-notification deadline and audit clause; updated to include Annexes and GDPR-compliant structure.
July 2026	Added Controller-notification duty for potentially unlawful instructions (Section 2); clarified that the sub-processor list is a separately maintained, incorporated-by-reference document (Section 6); added billing basis for extraordinary assistance (Section 7); permitted ISO 27001 certification/audit reports in lieu of on-site audits and added Article 30 records-of-processing confirmation (Section 9); specified concrete safeguards and transfer impact assessment for the Thinkific (US) transfer (Section 11); clarified that the liability cap does not limit regulatory fines or data subject claims (Section 12); added a Contact Persons section (Section 14); expanded Annex 1 with access control, encryption at rest, penetration testing, and business continuity measures; added an optional formal signature block.

Acceptance

By using Abra's services or signing the Main Agreement, the Controller agrees to this DPA. A signed copy may be requested if required for compliance purposes.