

Data Processing Agreement

Effective 29 August 2026. A later edit replaces this page in place.

This Data Processing Agreement (the “DPA”) forms part of the contract between **mvdm.io** and the customer organisation that uses a covered Product (“Customer”). It covers processing of personal data under the EU General Data Protection Regulation (EU GDPR) and the UK GDPR.

- **Legal name:** mvdm.io
- **Legal form:** sole proprietorship (eenmanszaak)
- **Chamber of Commerce (KvK):** 86594737
- **VAT identification number:** NL000000000B00 (placeholder — VAT number not yet issued)
- **Registered address:** De Vierakkers 15, 7766 BL Nieuw-Schoonebeek, the Netherlands
- **Email:** michiel@mvdm.io

1. Roles and scope

This DPA covers **mvdm.io Compliance**, **mvdm.io Translation Tools**, **mvdm.io Health Check** and **mvdm.io Statistics** (each a covered “Product”). **mvdm.io Commonplace falls outside this DPA:** for Commonplace, mvdm.io decides the purposes and means of processing itself, so there is no customer organisation to instruct it, and mvdm.io is controller rather than processor.

mvdm.io is the processor for personal data that Customer stores in a covered Product — including, depending on the Product, People and free text, translation text, browser screenshots, and Customer’s own end users — when Customer determines the purposes and means of that processing.

mvdM.io is the controller for sign-in and account administration, billing, first-party request analytics, and the public marketing site. That controller processing is described in the [Privacy Notice](#), not in this DPA's processor instructions.

2. Subject matter and duration

Subject matter: hosting and operating the covered Products so Customer can use them. Duration: for as long as Customer has a current licence for a covered Product, plus the closed-licence retention period below, unless the parties agree otherwise in writing.

3. Nature and purpose of processing

mvdM.io processes personal data in a covered Product only to provide that Product — including storage, display, search, and, for mvdM.io Compliance, assistant features and import extraction — and to support Customer on request. mvdM.io does not process that data for its own marketing.

4. Types of data and data subjects

Data categories depend on the covered Product:

- **mvdM.io Compliance:** workforce records and free text that Customer keeps in policies, registers, evidence, imports, and assistant conversations. Anyone on the account can read a Person's notes; Compliance has no field-level permission model.
- **mvdM.io Translation Tools:** translation text that Customer submits for translation.
- **mvdM.io Health Check:** browser screenshots of Customer's sites, including pages behind a sign-in that Customer has configured Health

Check to reach; the hostnames Customer submits for checking are also sent to Qualys SSL Labs for TLS grading.

- **mvdM.io Statistics:** Customer's own end users — the visitors to Customer's site or application that Statistics measures.

Data subjects are the people Customer includes in a covered Product: employees, contractors, end users, and others Customer records or exposes to it.

5. Customer instructions

Customer instructs mvdM.io to process personal data in a covered Product as needed to provide that Product and as Customer directs through it. mvdM.io will not process that data for other purposes except as required by law. If an instruction appears to infringe EU GDPR or UK GDPR, mvdM.io will inform Customer.

6. Confidentiality

People authorised to process personal data in a covered Product for mvdM.io are under confidentiality obligations.

7. Technical and organisational measures

mvdM.io implements the following technical and organisational measures:

- transport encryption for access to the applications;
- bcrypt password hashing;
- account-scoped tenancy so one customer's data is not served to another customer's users;
- sign-in through one dedicated service;
- hosting on a dedicated server in Germany;
- application logs kept for 7 to 14 days;

- deletion of an account's data for a Product after the closed-licence retention window, described in section 12, when no current licence remains.

Data is not encrypted at rest, and mvdm.io keeps no separate copy of it for recovery. If data in a covered Product is lost or corrupted, there is nothing else to restore it from. Customer should assess that risk on this basis rather than assume otherwise. A Platform Administrator may read mvdm.io Compliance and mvdm.io Translation Tools assistant conversations for support and quality.

8. Subprocessors

Customer authorises mvdm.io to use the subprocessors listed on the public [Subprocessor list](#). That page is incorporated by reference. mvdm.io remains responsible for subprocessors' performance of the processing obligations under this DPA. mvdm.io emails account owners when the Subprocessor list changes. A Customer who objects to a new subprocessor may end the contract, with no refund for time already paid, as described in the [Terms of Service](#).

9. International transfers

Application hosting is a dedicated server in **Nuremberg, Germany**. The following subprocessors process relevant data in the **United States**: **Stripe** (payments), **Cloudflare** (DNS, TLS proxy, and email), **xAI** (assistant and translation content), **Anthropic** (mvdm.io Compliance import extraction), and **Qualys SSL Labs** (mvdm.io Health Check hostname submissions for TLS grading). Transfers to these providers rely on their own standard contractual clauses. mvdm.io Commonplace's subprocessor, Google Books, does not appear here because mvdm.io Commonplace sits outside this DPA entirely (see section 1); it is disclosed on the [Subprocessor list](#) instead.

10. Artificial intelligence subprocessors

The mvdm.io Compliance and mvdm.io Translation Tools assistants send relevant content to **xAI**. Compliance's import extraction sends relevant content to **Anthropic**. This DPA does not promise that those providers never use content to train models.

mvdm.io Health Check offers optional Azure telemetry that connects to **Customer's own** Azure tenant. Microsoft is not a subprocessor of mvdm.io for that telemetry.

11. Assistance, breach, and audits

Taking into account the nature of the processing, mvdm.io will assist Customer with data-subject requests, security, breach notification, and data-protection impact assessments where reasonably possible through the product or by email. mvdm.io will notify Customer without undue delay after becoming aware of a personal-data breach affecting Customer's data in a covered Product. Audit rights are exercised reasonably, no more than once per year unless a breach or competent authority requires otherwise, and in a way that does not compromise other customers' security.

12. Return and deletion

Until a full product export exists, Customer may request return of its data for a covered Product by email to michiel@mvdm.io, during an active licence for that Product or the retention window. When a covered Product's licence ends, mvdm.io keeps that account's data for that Product for **365 days** from the licence end date. If Customer obtains a new current licence for that Product within those 365 days, the countdown stops and the data remains. If Customer does not, mvdm.io deletes that account's data for that Product after 365 days. Customer's sign-in account and users are not deleted by that wipe. This rule is the same for every covered Product.

13. Changes to this DPA

mvdm.io may replace this DPA by publishing an updated page with a new effective date. **Continued use of a covered Product after a replacement is acceptance of the replacement.**

14. Governing law

This DPA follows the governing law of the Terms of Service, without prejudice to mandatory data-protection rules.