

Data Processing Agreement (DPA)

Pursuant to Art. 28 Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), based on the model texts of the German data protection supervisory authorities and adapted to Platte's platform.

Version 1.0 · As of 29 October 2026

Informational translation. The German version is the legally binding one; in case of any discrepancy, the German text prevails.

between

Platte Software UG (haftungsbeschränkt)

Am Krögel 2
10179 Berlin
Germany

represented by the managing directors: Lucas Oliver Pilzen, Friedrich Theodor Gies

E-Mail: hello@platte.ai

– hereinafter „Platte“ or „Processor“ –

and

the respective customer under the General Terms and Conditions (GTC) of Platte Software UG (haftungsbeschränkt); the name and address follow from the underlying contract or the order confirmation.

– hereinafter „Customer“ or „Controller“ –

together „the Parties“.

Preamble

This Agreement is an annex to the GTC and governs the processing of personal data in connection with the provision and operation of a dedicated instance of the platform in the Platte Managed Cloud. In the case of self-hosting under § 6 of the GTC, the Customer is itself the controller for the processing carried out in its infrastructure; this Agreement does not apply there to the extent Platte has not taken over operation as a managed service. The processing of contract and payment data for receivables management is the sole responsibility of Platte as controller and is not subject to this Agreement.

§ 1 Subject matter and duration of the assignment

(1) Platte provides the Customer with the services under the main contract (GTC): the provision and operation of a dedicated instance of the Platte AI platform – chat application, inference via the Platte Privacy Gateway, runtime environment for agentic processes – for access over the internet on European infrastructure.

(2) As Platte processes personal data on behalf, on the instructions and in the interest of the Customer, or access to personal data in the performance of the services cannot be ruled out, the service is provided as commissioned processing under the German and European data protection laws applicable to the Customer.

(3) This Agreement is an annex to the GTC and becomes part of the main contract upon the Customer's acceptance of the GTC; a separate signature is not required for this. On request, the Parties will produce a separate signed version. The Agreement applies for as long as Platte processes personal data on behalf of the Customer. It does not end before the return and deletion obligations under § 10 of this Agreement have been fulfilled.

§ 2 Scope, nature and purpose of the processing, types of data and data subjects

The scope, nature and purpose of the data processing, the types of data and the circle of data subjects are set out in Annex 1. Automated decision-making, including profiling, pursuant to Art. 22 GDPR does not take place in Platte's area of responsibility.

§ 3 Technical and organisational measures

(1) Platte undertakes to take appropriate technical and organisational measures that reflect the state of the art (Art. 32 GDPR) for the data processed. The current measures – structured by physical access, system access, data access, disclosure, input and availability control, data secrecy, separation control, integrity and confidentiality, and procedures for regular review – are described in Annex 2.

(2) The data security measures may be adapted during the term of the assignment as part of technical and organisational development, provided the level of security does not decrease. Platte will agree material changes with the Customer in text form.

(3) Platte maintains a record of processing activities for the data processed on behalf of the Customer (Art. 30 (2) GDPR) and makes it available to the Customer on request. In addition, Platte provides a comprehensive and current data protection and security concept for the commissioned processing on request.

§ 4 Rectification, erasure, blocking and restriction of data

Platte may only rectify, erase, restrict or block the data processed on behalf of the Customer if the Customer instructs it to do so. Through the functions granted to it in the instance (including the management of sessions, users, stored content and exports), the Customer may also carry out rectifications and erasures itself. Platte does not make copies or duplicates of the data without the Customer's knowledge; this excludes proper data backups and the logging permitted under § 8 (4) of the GTC for billing, abuse detection and operational security.

§ 5 Obligations of the Processor

(1) Platte is aware of the relevant data protection provisions. It organises its internal operations in such a way that they meet the particular requirements of data protection.

(2) Platte familiarises the employees involved in carrying out the work with the data protection provisions relevant to them and obliges them to data secrecy and confidentiality (Art. 28 (3) lit. b GDPR, § 26 BDSG). This obligation continues after the end of the employment relationship. Platte demonstrates these obligations in an appropriate form on request.

(3) The data processed on behalf of the Customer is strictly separated from other data sets; each customer receives a dedicated, logically isolated instance.

(4) A data protection officer need not be appointed at Platte under § 38 BDSG. The contact person for data protection is Friedrich Theodor Gies (friedrich@platte.ai).

(5) Platte processes personal data on behalf of the Customer exclusively within the scope of the GDPR; the platform is operated on servers within the European Union. Transfers to third countries within the meaning of Art. 44 et seq. GDPR do not take place under this Agreement. The service providers engaged are listed in Annex 3.

(6) Platte supports the Customer with all statutory information and disclosure obligations connected with the commissioned data processing. Platte may provide information to data subjects or third parties only on the Customer's prior instruction. If a data subject asserts their rights directly against Platte, Platte forwards the request to the Customer without undue delay.

(7) Platte supports the Customer with any required data protection impact assessments.

§ 6 Sub-processors

(1) Platte may engage sub-processors for the processing of the Customer's data only with the Customer's consent. The sub-processors engaged at the time the Agreement is concluded are listed in Annex 3; by consenting to this Agreement, the Customer approves their engagement.

(2) If Platte intends to engage a further sub-processor or to materially change an existing engagement, it will inform the Customer in text form at least 30 days before the planned engagement (Art. 28 (2) GDPR). The information is additionally provided by publishing the updated Annex 3 in the Trust Center at platte.ai/sicherheit. The Customer may object to the change for data protection reasons within 30 days of receiving the information; if no objection is made in due time, the change is deemed approved. If the Parties do not reach agreement on an objection, the Customer has the extraordinary right of termination under § 13 (2) of the GTC.

(3) Platte imposes the obligations of this Agreement on the sub-processor to the extent required and ensures that the contractual arrangements with the sub-processor meet the data protection requirements in the contractual relationship between the Customer and Platte. Platte regularly reviews the sub-processor's compliance with the contractual obligations and documents this.

(4) Services that Platte obtains from third parties as ancillary services to support the performance of the assignment are not sub-processing relationships within the meaning of this provision, provided that access to personal data is not to be expected. In this respect too, Platte makes appropriate and legally compliant contractual arrangements and control measures.

§ 7 The Controller's rights of control

(1) Platte provides the Customer with verifiable guarantees of compliance with data protection law (e.g. self-declarations, information, attestations and certificates of the service providers engaged).

(2) The Customer, or a person commissioned by it, is entitled to review compliance with data protection provisions and the contractual arrangements to the extent required, in particular by obtaining information and inspecting the documentation of the technical and organisational measures. The platform's source code is published as open source and can be used for verification.

(3) The Customer will carry out reviews only to the extent required and will not disproportionately disrupt Platte's operations in doing so; reviews will be announced in good time.

§ 8 Incidents to be reported by the Processor

(1) Platte will inform the Customer without undue delay of disruptions to operations that entail risks for the Customer's data, as well as of any suspicion of data protection breaches in connection with the Customer's data. The same applies if Platte establishes that the security measures it has taken do not meet the statutory requirements.

(2) Notifications of a personal data breach to the Customer are made in text form and contain a description of the nature of the breach, where possible information on the categories and number of affected data records, the likely consequences, the name and contact details of a contact person, and an explanation of the measures taken to remedy the breach and mitigate possible adverse effects.

§ 9 Instructions of the Controller

(1) The Customer has the right to give Platte instructions on the nature, scope and procedure of the data processing. Instructions are given in text form; instructions given orally are documented by Platte.

(2) Platte processes the personal data processed on behalf of the Customer exclusively in accordance with the Customer's instructions and within the framework of the arrangements made. If Platte is of the opinion that an instruction infringes data protection law, it will inform the Customer without undue delay (Art. 28 (3) subparagraph 2 GDPR).

(3) The Customer will inform Platte without undue delay if it discovers errors or irregularities when reviewing the results of the assignment.

(4) As between the Parties, the Customer is responsible for the lawfulness of the processing of the personal data it enters and of the instructions it gives. If a third party asserts claims against Platte in connection with the processing of the Customer's data, the Customer shall indemnify Platte against such claims to the extent that they are based on a breach by the Customer of this Agreement or of applicable law. The indemnity does not apply to the extent that the claim is based on a breach by Platte.

§ 10 Termination of the assignment

- (1) This Agreement depends on the existence of the underlying main contract (GTC). If the main contract ends, this Agreement also ends without the need for separate termination.
- (2) The Customer may terminate the main contract without notice if Platte commits a serious breach of the provisions of this Agreement or of statutory provisions of the data protection laws applicable to the Customer and continuation of the commissioned processing until expiry of the notice period cannot reasonably be expected of the Customer.
- (3) After termination of the commissioned data processing, Platte will make the Customer's instance data available for export on request for a transition period of 30 days in a common, machine-readable format; the data is then erased unless statutory retention obligations exist (§ 11 (4) of the GTC). Platte confirms erasure to the Customer in text form on request. The Customer's data carriers and data sets are not subject to any right of retention by Platte; the Customer's right to data export is also unaffected by a temporary suspension of service under § 9 (4) of the GTC.
- (4) Platte is obliged to treat all knowledge of persons, trade secrets and data security measures obtained in the course of the contractual relationship confidentially, also after termination of this Agreement.

§ 11 Liability

Reference is made to Art. 82 GDPR. Otherwise, liability is governed by the provisions of the main contract (§ 15 of the GTC).

§ 12 Final provisions

- (1) The Parties undertake to treat all knowledge of trade secrets and data security measures of the respective other Party obtained in the course of the contractual relationship confidentially. This confidentiality obligation continues after termination of this Agreement.
- (2) If the Customer's property at Platte is endangered by measures of third parties (e.g. attachment or seizure), by insolvency proceedings or by other events, Platte must inform the Customer without undue delay.
- (3) Amendments and additions to this Agreement require text form. Platte may adapt Annex 2 (technical and organisational measures) in the course of technical development, provided the level of security does not decrease; Annex 3 (sub-processors) only in accordance with § 6 of this Agreement.
- (4) The law of the Federal Republic of Germany applies. The exclusive place of jurisdiction is Berlin, provided the Customer is a merchant, a legal entity under public law or a special fund under public law.
- (5) Should any provision of this Agreement be or become invalid, the validity of the remaining provisions shall not be affected. The invalid provision shall be replaced by a provision that comes closest to its economic purpose.
- (6) In the event of contradictions between this Agreement and the GTC or other agreements between the Parties, the provisions of this Agreement prevail for the commissioned processing.
- (7) This Agreement is drawn up in German. Only the German version is binding; an English translation is provided for information purposes only and creates neither rights nor obligations. The current German version is available at platte.ai/avv, the English informational version at platte.ai/avv-en.pdf. The version published at the time the contract is concluded is decisive; Annex 2 and Annex 3 are updated in accordance with this Agreement.
- (8) The Customer expressly agrees to this Agreement as part of the registration process; the consent covers the version published at that time, including its Annexes. Platte stores the version of the Agreement (version number and date), the time of consent and the associated account, and evidences the consent in text form on request.
- (9) Platte provides a version signed by both Parties on request.

Annex 1 – Scope, nature and purpose of the processing, types of data and data subjects

Subject matter of this Agreement is the following commissioned processing within the Platte Managed Cloud:

Purpose of the processing

- Provision, operation and support of the dedicated instance of the platform (chat application, inference via the Platte Privacy Gateway, runtime environment for agentic processes);
- Billing and management of usage quotas (seats, credits, top-up, pay-as-you-go API key);
- Abuse detection and operational security (logging under § 8 (4) of the GTC).

Nature of the processing

Storage, organisation, structuring, retrieval, reading, display, combination, transmission (to the EU inference providers named in Annex 3 via the Platte Privacy Gateway), logging, restriction, rectification and erasure.

Categories of data subjects

- The users of the instance set up and designated by the Customer (e.g. employees, authorised third parties);
- Persons contained in the content data (e.g. persons to whom documents, requests or attachments relate).

Categories of personal data

- Master data of user accounts: name, email address, user name and, in the case of organisation-based use, organisation and role membership;
- Authentication and security data: password hashes, personal access tokens (PAT), session information;
- Usage data: sessions, requests and consumption values (tokens, credits), models and features used, timestamps;
- Content data: prompts, uploaded documents and files, chat histories, stored knowledge and preferences, outputs; in the case of speech recognition also audio data for transcription purposes;
- Log data for billing, abuse detection and operational security.

Special notes

- To provide the inference services, content is transmitted via the Platte Privacy Gateway to the configured models at the providers in Annex 3. Platte does not use customer content to train models (§ 8 (2) of the GTC).
- Automated decision-making, including profiling, pursuant to Art. 22 GDPR does not take place.
- The processing of contract and payment data for receivables management is the sole responsibility of Platte as controller and is not subject to this Agreement.

Annex 2 – Technical and organisational measures (Art. 32 GDPR)

1. Physical access control

The platform is operated on servers in the data centres of the EU providers named in Annex 3; the providers exercise physical access control over the server sites.

2. System access control

Access to the platform requires authentication (one-time password and/or personal access tokens). Access without authentication is not possible.

3. Data access control

Within each instance there is a role and permission management system; administrative access is limited to the minimum required and is logged.

4. Separation control

Each customer receives a dedicated, logically isolated container instance with its own database; there is no shared tenant boundary. Code executions run in separate sandbox environments.

5. Disclosure control

Hosting and inference take place exclusively with providers within the European Union (Annex 3). Requests are transmitted via the Platte Privacy Gateway, which holds the provider keys; provider keys are not passed on to customers or third parties. Data processing agreements are in place with all service providers.

6. Input control

Requests are logged for billing, abuse detection and operational security (§ 8 (4) of the GTC).

7. Availability control

Operation on European infrastructure; backup function (full backup of database and files) together with export via the administration interface; documented restart procedures after disruptions.

8. Data secrecy

Employees are obliged to data secrecy and confidentiality (Art. 28 (3) lit. b GDPR, § 26 BDSG); the obligation continues after the end of the employment relationship.

9. Integrity and confidentiality

Encryption of data transmission (TLS); storage and processing exclusively within the EU infrastructure.

10. Procedures for regular review

Ongoing security updates; review of changes before release; regular internal review of the effectiveness of the measures; evidence is provided to the Customer on request.

Annex 3 – Sub-processors (as of 29 October 2026)

At the time the Agreement is concluded, Platte engages the following sub-processors:

Name	Location	Type of service
Scaleway SAS	Paris, France, EU	Hosting, LLM inference, email delivery
Hetzner Online GmbH	Gunzenhausen, Germany, EU	Hosting, LLM inference
TensorX Ltd.	Dublin, Ireland, EU; Helsinki, Finland, EU	LLM inference, speech processing (transcription, speech output)
Berget AI AB	Stockholm, Sweden, EU	LLM inference
Heinlein Hosting GmbH (mailbox.org)	Berlin, Germany, EU	Email hosting (mailbox, receiving and sending email)

The current list of processors is additionally published in the Trust Center at platte.ai/sicherheit; changes are subject to the information and objection rules under § 6 (2) of this Agreement and § 13 (2) of the GTC.