Data Processing Agreement

Last updated on: 2026-09-23

This Data Processing Agreement (“DPA”) applies to Opper’s provision of its AI integration platform and the associated services (collectively the “Services”) and form an integral part of the agreement between Opper and the Customer covering the Customer’s use of the Services. For pay-as-you-go customers, the Terms of Service | Opper AI govern your use, and for enterprise customers, the customer agreement governs your use (both referred to as the “Main Agreement” in this DPA, as applicable). Opper and the Customer are hereinafter also referred to as a “Party” and together as “Parties”. Any capitalized terms used herein shall have the same meaning as defined in the Main Agreement unless specifically defined otherwise in this DPA.

1 Background

1.1 As part of the Services provided in accordance with the Main Agreement, Opper will be processing certain personal data on behalf of the Customer. The Customer is the data controller and Opper is the data processor regarding the processing of personal data described herein.

1.2 This DPA governs the conditions for Opper’s processing of, and access to personal data in accordance with the General Data Protection Regulation (EU) 2016/679 (”GDPR”) and other relevant data protection legislation (all together ”Data Protection Legislation”).

1.3 The DPA consists of this document and the appendices. In the event of any contradictions between this document and the appendices or the Main Agreement, this document shall take precedence.

1.4 All terms defined in Article 4 of the GDPR shall have the same meaning in the DPA, unless expressly stated otherwise.

2 Scope of processing

2.1 For the shared Platform deployment, Opper deploys the web application and API service in the Amazon Web Services (AWS) Stockholm, Sweden region. Separately agreed dedicated or customer-hosted deployments may have different hosting locations. This does not mean that all processing connected with the Services takes place within the European Economic Area (“EEA”). Other processing, including billing and email delivery, may take place outside the EEA, as described in the Sub-processors list and Section 5.

Model inference may take place inside or outside the EEA depending on the model route used; it is not restricted to the EEA by default. The Customer may select models for its requests and, where Rules are available under its plan, restrict eligible routes for Customer-selected model calls based on the recorded inference and storage locations.

The personal data processed under this DPA (“Included Personal Data”) is described in the Annex: Categories of Data Subjects and Categories of Personal Data.

2.2 Opper shall only process Included Personal Data in accordance with the Customer’s written instructions, which are set out in this DPA, unless further processing is required under applicable EU or Member State law to which Opper is subject. In such case Opper shall inform the Customer of this legal obligation unless such disclosure is prohibited by law.

3 Security and assistance

3.1 Opper will apply suitable technical and organizational safeguards to protect Included Personal Data, as required under Article 32 of the GDPR. This includes implementing measures for preventing accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to the Included Personal Data. Opper's security measures are listed at https://opper.ai/security-overview.

3.2 Opper shall assist the Customer in fulfilling its obligations under Articles 32 to 36 in the GDPR, especially regarding the security of processing and personal data breaches. Opper shall notify the Customer without undue delay and within 48 hours after Opper has learned of a personal data breach affecting the Included Personal Data.

3.3 Opper will assist the Customer in meeting its obligations under Chapter III of the GDPR, including data subject rights such as access, deletion, correction, and data portability. Opper will notify the Customer without undue delay of any such requests from data subjects.

4 Sub-processing

4.1 Opper has the Customer's general authorization to engage sub-processors for the processing of Included Personal Data on behalf of the Customer ('Sub-processors'). Subprocessors that are necessary to run the Platform are listed here: Sub-processors | Opper AI.

4.2 In addition, Customer can configure which AI models to use on the Platform. Relevant subprocessors then vary depending on Customer's own configurations. All configurable subprocessors are also listed at: Sub-processors | Opper AI.

4.3 The list provided at: Sub-processors | Opper AI will be continuously updated as new model providers are added to the Platform. For any sub-processors, Opper enters into a sub-processing agreement with the same obligations as in this DPA. Opper shall be fully liable for the actions and performance of any Sub-processors engaged in the processing of Included Personal Data on behalf of the Customer.

4.4 Opper shall notify the Customer through the Services at least 30 days in advance of any intended addition or replacement of a Sub-processor. The Customer is responsible for regularly checking the Service for such updates. The Customer is entitled to object to such changes, based on objective grounds relating to the security of the processing under the DPA. If the Customer makes an objection and Opper does not accept to replace the Sub-processor or refrain from using it, either Party is entitled to terminate the affected service, by giving the other Party 30 days' written notice.

5 Third country transfers

The Processor shall process Personal Data within the European Union/European Economic Area, or in a third country that is subject to (i) an adequacy decision under Article 45 GDPR, or (ii) appropriate safeguards under Article 46 GDPR (such as Standard Contractual Clauses).

6 Confidentiality

6.1 Opper shall restrict access to Included Personal Data solely to those of its employees, representatives and Sub-processors who require access for the sole purpose of providing the Services. Opper shall ensure that all such employees, representatives and Sub-processors are bound by confidentiality, either through commitment or statutory obligation.

6.2 Opper shall not disclose Included Personal Data or any information related to its processing under this DPA to third parties without express instruction from the Customer. This obligation excludes:

(i) Disclosure to Sub-processors for fulfilment of their obligations under a sub-processing agreement,

(ii) information that is publicly known (due to other reasons than a breach of the DPA),

(iii) information compelled by mandatory law or regulation. In such cases, Opper shall promptly inform the Customer and request guidance.

6.3 The confidentiality obligations herein shall apply without limitation in time.

7 Audit and inspection

Opper shall without undue delay make available to the Customer upon the Customer's request, all information necessary to demonstrate that Opper is fulfilling its obligations under the DPA and the relevant Data Protection Legislation. Opper shall also enable and assist in audits, including inspections, which are conducted by the Customer or by a third party authorised by the Customer, at the Customer's cost. Upon the Customer's request, Opper will provide the Customer with information necessary to show that Opper is meeting its obligations under the DPA. Opper will cooperate with audits or inspections, which will occur no more than once a year and will be notified at least 10 business days in advance. These audits or inspections will be conducted by the Customer or an authorized third party, at the Customer's cost.

8 Term and termination

8.1 The DPA shall remain in force as long as Opper processes personal data on behalf of the Customer, according to the Main Agreement between Opper and the Customer.

8.2 Opper shall upon termination of the Main Agreement or upon notice from the Customer, at the Customer's choice, return or delete all Included Personal Data processed under the DPA, unless Opper is required to retain the Included Personal Data to comply with mandatory law or regulation.

8.3 Unless otherwise instructed by the Customer, Opper will delete Included Personal Data after 30 days from termination or expiry of the Main Agreement.

9 Notices

Unless otherwise specified, all notices under this DPA must be in writing and sent by email. Notices to Opper must be sent to support@opper.ai. Notices are deemed received on the date of transmission, provided the sender does not receive a delivery failure message. Either Party may change its email address for notices by providing written notice to the other Party.

10 Compensation

Opper shall be entitled to reasonable compensation for all work and all costs that arise due to the Customer's instructions for processing if these exceed the features and level of security that Opper normally applies on its services or provides to its customers, e.g. in the case that Opper's systems and/or Services require special adjustments or development following special requests from the Customer. Opper is not entitled to compensation for costs which arise based on compliance with requirements under the relevant Data Protection Legislation.

11 Liability and indemnification

Subject to mandatory law, the limitations of liability set out in the Main Agreement shall apply to this DPA. Notwithstanding the above, the Parties acknowledge that each Party shall bear any administrative fines pursuant to GDPR Article 83 imposed on the Party by the relevant supervisory authority.

12 Governing law and dispute resolution

This DPA shall be governed by the substantive law of Sweden. Disputes arising from this DPA shall be finally settled in accordance with the resolution of disputes clause stated in the Main Agreement.

Categories of Data Subjects and Categories of Personal Data

Annex to the Data Processing Agreement ("DPA") between customer as the Controller and Opper AI as Processor.

This Annex describes, for the purposes of Article 28(3) and Article 30 GDPR, the categories of data subjects and the categories of personal data processed by the Processor on behalf of the Controller in connection with the Services.

A. Categories of Data Subjects

Category	Description
Controller's authorized users	Employees, contractors, or other individuals authorized by the Controller to access, administer, or use the Service (e.g. account administrators, developers, API key holders).
Individuals identified in Input content	Any data subject whose personal data is contained within the prompts, files, or other content (“Inputs”) submitted to the Service by or on behalf of the Controller. The specific individuals depend entirely on the Controller's use case and may include, without limitation, the Controller's customers, employees, job applicants, end users, or other third parties referenced within such content.
Individuals identified in Output content	Any data subject whose personal data appears within the content generated by an AI Model in response to an Input (“Outputs”), to the extent such Outputs contain or reproduce personal data.

B. Categories of Personal Data

Category	Description
Account and administrative data	Name, business contact details (email, phone), job title, login credentials, API keys or access tokens, billing and payment details, and IP address of the Controller's authorized users.
Usage and technical/metadata	Timestamps, request and response metadata, session identifiers, device and browser information, the AI Model selected, token/usage counts, and system or error logs generated through use of the Service.

Input content (Controller-determined)	Any personal data contained within the Inputs submitted by the Controller. Because Input content is determined solely by the Controller, this may include ordinary categories of personal data (e.g. names, contact details, identification numbers, professional information) and, where applicable, special categories of personal data under Article 9 GDPR or personal data relating to criminal convictions and offences under Article 10 GDPR, subject to Art 9 Appendix (Special Category Data).
Output content (derived)	Personal data generated, summarized, or reproduced within Outputs returned by an AI Model in response to an Input, which may mirror or otherwise reflect personal data contained in the corresponding Input.

Where the Controller's use of the Service involves special categories of personal data within the meaning of Article 9 GDPR, the terms of Art 9 Appendix (Special Category Data) apply in addition to this Annex.