

Data Processing Agreement

Data Processing Agreement

10th of September 2025

Definitions

Words or expressions defined in **"quotation marks"** have the same meanings each time they are used in this DPA. Unless we say otherwise below, any words or expressions that are defined in the Terms of Service and the Privacy Policy have the same meanings when used in this DPA too.

- **"Applicable Data Protection Law"** means all laws and regulations applicable to Prisma's processing of Relevant Data under, including the GDPR, the UK GDPR, the California Consumer Privacy Act (CCPA/CPRA), and any other relevant data protection legislation.
- **"Personal Data", "Special Categories of Personal Data", "Controller" and "Processor"** have the meanings.
- **"Relevant Data"** means personal data data as described in the annex below.
- **"Prisma", "we", "us" or "our"** means Prisma Data, Inc., a Corporation registered in Delaware, USA.

Relationship between you and Prisma

1. To the extent that Prisma provides access to its products and services to you and you are a Controller of any Relevant Data under GDPR, then you (the Controller) appoint Prisma as a Processor to process that Relevant Data.
2. This DPA will apply to you and us for as long as our Terms of Service apply to you, or for as long as we process Relevant Data on your behalf - whichever is longer.

Instructions

1. You instruct Prisma to process the Relevant Data in accordance with this DPA and only for the purpose described in the annex below (or as otherwise may be agreed between you and Prisma in writing) (the "**Purpose**"). Prisma may not process the Relevant Data for any other purpose, unless it is required to under EU law, EU member state law or US law. In that case, Prisma will write to you about why it needs to process the Relevant Data, unless it is restricted by law from informing you.
2. If Prisma believes that an instruction given by you violates the Applicable Data Protection Law, Prisma will let you know immediately.
3. Prisma is not currently aware of being subject to legislation that would prevent it from fulfilling the DPA, but it will let you know without undue delay if that changes or is expected to change.

Transfers of Relevant Data

1. Prisma may transfer Relevant Data outside of the European Economic Area, UK or Switzerland under the 2021 Standard Contractual Clauses (SCCs) adopted by the European Commission, the UK International Data Transfer Agreement (IDTA), or any successor instruments to sub-processors once it has taken necessary measures to ensure that the sub-processor has an appropriate Data Processing Agreement and complies with the Applicable Data Protection Law. These measures may include transferring the Relevant Data to a recipient in a country that the European Commission has decided provides adequate protection for personal data or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission.
2. Prisma is committed to the EU-US Data Privacy Framework, UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, as dictated in our Privacy Policy.
3. Prisma will conduct Transfer Impact Assessments (TIAs) where required.

Prohibited data

1. You agree that you won't disclose to Prisma for processing any Personal Data for which you do not have the rights, permissions or consents required

under Applicable Data Protection Law to enable Prisma to lawfully process it.

Confidentiality

1. Prisma will ensure that any person that it authorises to process the Relevant Data will keep the Relevant Data confidential under a statutory obligation of confidentiality or other commitment.

Security practices

1. Prisma currently abides by strict technical and organisational security practices.
2. Prisma may change these measures from time to time, but will always maintain appropriate technical and organisational measures that ensure a level of security appropriate to the risk and protect the Relevant Data from being:
 - accidentally or unlawfully destroyed, lost or altered,
 - disclosed or made available without authorisation, or
 - otherwise processed in violation of the Applicable Data Protection Law.
3. Prisma will also comply with any other applicable data security requirements that are directly imposed on it, including the data security requirements of the country in which Prisma is established and where the data processing will be performed.
4. The appropriateness of the technical and organisational security measures will be based on:
 - the current state of the art;
 - the cost of their implementation; and
 - the nature, scope, context and purposes of processing, as well as the likelihood of risks and the impact on the data protection rights and freedoms of data subjects.
5. On your request, Prisma will provide you with sufficient information to enable you to check that Prisma is complying with its obligations under the

DPA, including that it has implemented the technical and organisational security measures described above.

6. Prisma maintains compliance with recognized industry standards, including ISO 27001 and SOC 2 Type II, where applicable.

Audit

1. You may at your own cost appoint an independent expert who (so long as the expert isn't a competitor of Prisma) will be given access to the information necessary to audit whether Prisma complies with its obligations under the DPA - including whether the appropriate technical and organisational security measures have been implemented.
2. You'll need to let us know at least 28 days before you want your expert to have access. And, before we give them access, they'll need to enter a customary non-disclosure agreement with Prisma that ensures that they treat all information they obtain or receive from Prisma and/or its affiliates confidentially and may only share that information with you.
3. Any findings or reports created on the basis of the expert's inspection and audit must be shared with Prisma and will be treated as confidential information.

Requests from authorities

1. Prisma will give authorities, which have a right under EU law, EU member state law or US law to enter your suppliers' facilities, access to Prisma physical facilities, provided that their representatives can show proper proof of identity.
2. Prisma must, without undue delay after becoming aware of the facts, notify you in writing about any request from an authority for disclosure of the Relevant Data, unless Prisma is expressly prohibited from informing you under EU law, EU member state law or US law.

Security incidents

1. Prisma shall, without undue delay and within 72 hours of becoming aware of the facts, inform you in writing about any suspicion or finding of a

personal data breach, in accordance of Article 33 of the GDPR.

- a. A personal data breach can be any security event that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Relevant Data transmitted, stored or otherwise processed by Prisma; and
- b. any other material failure to comply with Prisma obligations under this DPA.

Cooperation and data subjects' rights

1. Prisma will assist you with the handling of any requests from data subjects under the GDPR and, where commercially practicable, under any other Applicable Data Protection Law, including requests for access, rectification, blocking or deletion, which relates to our processing of the Relevant Data, normally within 30 days.
2. If Prisma receives such a request, Prisma will not respond to it other than to inform the requesting data subject:
 - whether a review invitation email has been sent to the data subject on your behalf; and
 - that he/she should submit his/her request to you, given that you will be responsible for responding to these requests.
3. Prisma will assist you with meeting the other obligations that may be imposed on you under EU law, EU member state law or US law related to data processing where our assistance is necessary for you to comply with your obligations. This includes providing reasonable cooperation to you in connection with any data protection impact assessment that may be required in accordance with article 35 and 36 of the GDPR.
4. Prisma will also provide information related to the provision of the services to authorities or your external advisors and auditors if this is necessary for the performance of their duties in accordance with EU law, EU member state law or laws in the US.
5. In the annex below, Prisma has stated the servers, offices etc. used to provide the services under the [Terms & Privacy](#). You may request information about the servers, offices used by Prisma in connection with these services and Prisma will respond within 30 days.

6. Prisma may charge reasonable costs for excessive or manifestly unfounded requests.

Subprocessors

1. Prisma may engage third-party subprocessors to process the Relevant Data, provided that Prisma imposes data protection obligations on each subprocessor that require it to protect the Relevant Data to at least the same standard imposed on Prisma in this DPA. You can view a list of Prisma's current subprocessors at <https://trust.prisma.io/>.
2. Prisma will update this list and notify you via email when subprocessors are added or removed.
3. You can object to any additional or replacement subprocessor within 28 days of it being appointed, provided that your objection is based on objective and reasonable grounds relating to data protection. If Prisma chooses not to suggest an alternative subprocessor, or if you object to all of Prisma's alternative subprocessors, Prisma will work with you in good faith to find alternatives or you may terminate your subscription (if any) by giving us 14 days notice.
4. On your request, we will give you a copy of the data protection obligations in Prisma's agreement with the subprocessor.
5. Prisma will be liable for any breach of this DPA that is caused by an act, error or omission of one or more of its subprocessors.

Deletion or return of Relevant Data

1. Prisma will retain Relevant Data only as long as necessary for the purposes of processing or as required by law.
2. After these periods have ended, or on your earlier request, Prisma will immediately return or delete (including anonymised) the Relevant Data in a manner and form decided by Prisma, acting reasonably. This won't apply to the extent that Prisma is required by applicable law to retain some or all of the Relevant Data.
3. Prisma will confirm deletion or anonymisation in writing upon your request.

Data Protection Officer

Prisma has a subsidiary based in Germany acting as Prisma's Data Protection Officer. You can reach our data protection officer by sending an email to: dpo@prisma.io.

ANNEX

Purpose

- Providing users access to our platform, and integrations with your platform, for the users to manage and process their data.

Categories of data subjects

- Your customers / users and their respective data.
- Our customers / users and their respective data.

Categories of Personal Data

- Name
- Email address
- Account number(s)
- Any other Personal Data that is stored with Prisma through your use of Prisma's services.

Special Categories of Personal Data

Prisma does not intentionally collect or process any Special Categories of Personal Data, as it is not needed for the purposes of providing you or your users access to our services. However, Special Categories of Personal Data may be processed if you or your users choose to include this data within their profiles, databases, or other linked services.