Data Processing Agreement

between

Crismo GmbH

Prenzlauer Allee 186

10405 Berlin

Germany

(hereinafter "Processor")

and

Customer

Address

(hereinafter "Controller")

(both parties together hereinafter referred to as „Parties“)

Preamble

This contract shall govern the processing of personal data on behalf of the Controller in the course of the use of Crismo software products (Software as a Services version) on the basis of one or more separate software licensing agreement(s) (hereinafter individually and collectively referred to as the “Agreement”). By entering into the Agreement, the Parties have constituted a contractual relationship regarding the processing of personal data on behalf of the Controller with respect to Art. 28 GDPR (“Processing”). In order to specify rights and obligations in accordance with applicable laws, the Parties enter into this DPA in the light of the fact that the terms “Controller” and “Processor” are defined in Art. 4 section 7 and Art. 4 section 8 GDPR.

1 Applicability

This DPA applies to all works which lie within the scope of the Agreement and are subject to the processing of personal data by the Processor or a Sub-Processor, subsequent to their transfer from the Controller to the Processor in whatever form (this kind of personal data hereinafter referred to as “Data”). This DPA including its attachments shall explicitly not apply in case that the Controller directs the Processor to store its Data on servers outside of the European Union or the European Economic Area (EEA). Any such processing outside of the European Union or the European Economic Area requires a separate written agreement between the Parties. The Controller's optional use of the AI feature “Crismo AI” is not affected by the foregoing and is governed by Attachment 3.

2 Scope of Work

(1) The scope and the duration of the Processing as well as range, type, and purpose of the intended Processing of Data are set out in the Agreement.

(2) The following types and categories of Data are subject to the collection, processing and/or use by the Processor: user data (first and last name, complete postal address, e-mail address, company name), access and authentication data (e.g. username, hashed password, single sign-on login information), IP-address of each access, business process models/organigrams/diagrams including extended attributes, comments to business process models/organigrams/diagrams, contents of any optionally transferred Data, workflow status information, process log-files including business data.

(3) The group of persons affected by the Processing of their Data includes: on the Controller's side: user of the systems (modeling users, invited persons, hub users), e.g. employees, customers or business partners of the Controller, as well as further persons whose Data are included in user data (business process models/organigrams/workflows, files, transferred process log-files including business data) (if any).

(4) The Processing of special categories of personal data within the meaning of Art. 9 GDPR is not the subject matter of this DPA. The Controller shall ensure that it does not transfer any such data in the course of using the Crismo products, unless the Parties agree otherwise in writing.

3 Responsibilities and Authority to Instruct

(1) In particular, the Controller shall be responsible for the legitimacy of Data transfer to the Processor. The Controller shall be entitled to demand to hand over, rectify and erase Data as well as to restrict the Processing at any time.

(2) The Processor shall process Data solely in compliance with the Controller's instructions. An instruction shall be understood as a specific order in written form (e-mail is sufficient) that is related to the Processor's work with Data. Instructions shall be defined initially by the Agreement and they can subsequently be adjusted, complemented or replaced by the Controller.

(3) Copies and duplicates shall not be created without the knowledge of the Controller. The aforementioned shall not apply to Backups as long as they are required to ensure the proper Processing and it shall not apply to Data which have to be retained due to the compliance with legal requirements.

(4) If the Processor is of the opinion that an instruction violates data protection regulations, it shall notify the Controller forthwith. The Processor shall be entitled to suspend the execution of such instruction as long as this has been confirmed or adjusted by the Controller.

(5) The Processor shall disclose Data to third parties or data subjects solely after prior approval by the Controller. Should a data subject contact the Processor directly to exercise its rights (in particular access, rectification, erasure, restriction of processing, data portability, or objection), the Processor shall forward such request to the Controller forthwith. The Processor shall support the Controller, to the extent reasonably possible and within a reasonable scope, by appropriate technical and organizational measures for fulfilling the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

(6) The Processor shall use reasonable efforts to support the Controller with the fulfillment of its obligations under Art. 32 to 36 GDPR. This includes in particular support regarding data protection impact assessment. The Processor shall be entitled to a remuneration for support services which lie not within the scope of the Agreement or which have not been caused through the Processor's misconduct.

(7) The Processing generally takes place in member states of the European Union or in a state party to the Agreement on the European Economic Area. This is without prejudice to occasional, narrowly limited access by support or maintenance personnel of a Sub-Processor from a third country where required in an individual case (e.g. for short-term troubleshooting), provided that appropriate safeguards within the meaning of Art. 46 GDPR (in particular Standard Contractual Clauses) have been agreed for this purpose and such access is limited to what is strictly necessary to perform the relevant task. Any further relocation of the Processing to a different state requires the Controller's prior approval. The Controller's optional use of the AI feature "Crismo AI" is governed, by way of exception, by Attachment 3.

(8) The Processor ensures that all persons who are authorized for the Processing are bound by an obligation of confidentiality.

(9) Insofar as the Processor is legally obliged to do so pursuant to Art. 37 GDPR or § 38 BDSG, it shall appoint a Data Protection Officer who is entrusted with the relevant tasks. The Processor's data protection contact can be reached via contact@crismo.io.

(10) The Controller shall be notified forthwith regarding checks and measures by regulatory authorities, provided that those are related to the Processing under this DPA.

4 Technical and Organizational Measures

(1) The Parties agree upon the technical and organizational measures defined in Attachment 1, according to Art. 28 (3) lit. c) GDPR in conjunction with Art. 32 GDPR. Where the Controller uses the optional AI feature "Crismo AI", the measures set out in Attachment 3 apply in addition.

(2) Technical and organizational measures are subject to technical progress. Thus, the Processor shall be entitled to implement equivalent measures as an alternative. However, the security level of the measures set out in Attachment 1 must not be decreased. Significant adjustments shall be documented.

(3) The Processor shall provide the Controller with any relevant information that is necessary to demonstrate its compliance with statutory and contractual requirements according to this DPA. If this requires audits to be to carried out by the Controller or an authorized auditor (which shall not be a direct or indirect competitor of the Processor), the Processor shall allow such audits and use reasonable efforts to facilitate their performance, provided that any audit shall be performed at a minimum level of disturbance with regard to the Processor's business operations. The Processor's evidence of appropriate measures' implementation shall substitute the aforementioned audits, provided that the Processor is able to provide an appropriate attestation on the basis of reports from properly qualified and independent third parties (e.g. auditors, external data protection officers, IT security department, data protection auditors) or an appropriate certification through IT security or data protection audit.

(4) An audit in accordance with section (3) above can be performed at any time after prior agreed appointment and during the Processor's normal business hours but not more than once a year if no suspicion with regard to a breach of this DPA exists.

5 Notification in Case of Breach by the Processor

(1) In the course of the Processing, the Processor shall notify the Controller forthwith in case of a severe disruption of its business operations, suspicion of breach of contractual or statutory data protection regulations, actual breaches of the latter, or other irregularities. Notification shall be made without undue delay, generally within 48 hours of becoming aware of the incident, to enable the Controller to comply with any applicable statutory reporting deadlines, in particular under Art. 33 GDPR.

(2) In coordination with the Controller, the Processor shall take appropriate measures to protect Data and to mitigate possible negative effects for data subjects.

6 Erasure and Return of Data

(1) Transferred data carriers and datasets will remain the Controller's property.

(2) After completion of the contractually agreed services or earlier, after request by the Controller, but not later than the termination of the Agreement, the Processor shall in the Controller's sole discretion return or destroy any documents, created works (either through Processing or use of Data) as well as databases (including copies and reproductions) that came into the Processor's possession in the course of the Processing. The same applies to test and scrap materials. The Controller shall be provided with a deletion report upon its prior request.

(3) The Processor shall be entitled to retain during the applicable retention period after termination of this DPA any documentation that serves to verify the Processor's compliance in the course of the Processing. Alternatively, such documentation can be returned to the Controller for discharge at the termination of this DPA. Likewise, back-up copies can be retained for a longer period than those mentioned in section (2) above, if their erasure outside of the routine erase cycles would cause disproportionate efforts for the Processor. However, the retention period of back-up copies shall not exceed 6 (six) months after the termination of the Agreement.

7 Sub-Processors

(1) In addition to those listed in Attachment 2, the Processor shall not engage any third parties for the processing of personal data ("Sub-Processors") without the prior written consent of the Controller. The engagement of the Sub-Processor named in Attachment 3 for the optional AI feature "Crismo AI" is governed by Attachment 3. Notwithstanding the foregoing, the Controller consents to the engagement of new Sub-Processors, provided that

(i) the Processor provides at least 30 (thirty) days' prior notice to the Controller of the engagement of such Sub-Processor;

(ii) the Processor and each Sub-Processor maintain a contractual relationship which ensures at least the same level of data protection as the one provided by this DPA, including compliance with all contractual and statutory regulations, in particular with regards to the implementation of technical and organizational measures to ensure proper protection levels in the course of the Processing; and

(iii) such Sub-Processor generally performs the Processing under this DPA within a member state of the European Union or in a state party to the Agreement on the European Economic Area; a narrowly limited access from a third country required in an individual case (in particular for support or maintenance purposes) is permitted, provided that appropriate safeguards within the meaning of Art. 46 GDPR have been agreed for this purpose.

Should the requirements (i) to (iii) above not be met, the Controller shall be entitled to object to the engagement of further Sub-Processors within 14 (fourteen) days after reception of the notification defined in (i) above. The Parties shall use reasonable efforts to reach an amicable solution in such case. If no agreement is reached within a further 30 (thirty) days, the Controller shall be entitled to terminate that part of the Agreement whose performance requires the use of the relevant Sub-Processor, subject to 30 (thirty) days' notice to the end of a calendar month.

(2) Ancillary services from third parties which serve to facilitate the Processing (e.g. telecommunication services, maintenance services) shall not be understood to be sub-processing in the meaning of this DPA. However, in order to ensure protection and security of the Controller's Data, the Processor shall be obliged to maintain proper and lawful contracts and control measures for ancillary services provided by third parties.

(3) With regard to the Controller's audit rights towards Sub-Processors, the Processor shall contractually agree with each Sub-Processor that the requirements set out in § 4 (3) of this DPA apply to the full extent.

(4) If a Sub-Processor fails to comply with its data protection related obligations, the Processor shall be liable vis-à-vis the Controller for that Sub-Processor's failure. Upon the Controller's request, the Processor shall cease partially or completely the engagement of that Sub-Processor or terminate the contractual relationship with that Sub-Processor if this is not unreasonable.

(5) As far as the contractually agreed Crismo Software includes functionality that is based upon the services of third parties, and if this functionality can be activated at the Controller's sole discretion, the respective third party shall solely become the Controller's contractual partner in terms of the use of such functionality. In this case, the terms of use as well as the data protection regulations of that third party shall apply exclusively. This DPA shall not govern the Controller's use of such functionality.

8 General Provisions

(1) Unless stipulated otherwise in this DPA, written form (e-mail) shall be sufficient for all declarations, in particular notifications. Modifications and amendments to this DPA must be made in written form (e-mail) as well.

(2) The Attachments "Technical and organizational measures", "Existing Sub-Processors" and "Crismo AI (optional)" form part of this DPA.

(3) In the event of any conflict between this DPA and the Agreement, the provisions of this DPA shall prevail with regard to matters of data protection.

(4) Should individual provisions of this DPA be or become invalid, in whole or in part, this shall not affect the validity of the remaining provisions.

9 Signatures

This DPA is executed by the Parties, or by their duly authorized representatives, as of the date(s) set out below.

Crismo GmbH	Customer
Place, Date:	Place, Date:
Signature:	Signature:
Name (in print):	Name (in print):
Position/Title:	Position/Title:

Attachment 1 - „Technical and Organizational measures“

1. Confidentiality

Administrative access control

All data centers commissioned by the Processor for the operation of production and backup systems are equipped with up-to-date physical access protection mechanisms. These include security guards, video surveillance and electronic access systems, including logging.

The data carriers used for storing Data are encrypted at the data carrier level with passwords that are considered to be secure according to the current state of technology, using up-to-date and secure encryption methods. Data center staff with authorized access to the hardware will not be able to access Data. They are also not aware of any access to the systems operated by the Processor.

For administrative access, the Processor always uses passwords with minimum lengths of 20 characters and secure connections (at least or equivalent to SSH, 2048 bits). All system passwords are changed after 12 months for security reasons. The administrative connection to the servers requires a second factor.

The public IP addresses used for the Processor's SaaS solutions allow access only via the HTTP, HTTPS, and SMTP application protocols.

Access control

A strict need-to-know and principle of least privilege restriction is applied for every system and Data access. Access rights are granted based on job responsibilities. Access to the administrative interface for support staff is protected by dual authentication (HTTP and application level) and secure connection. All employees with access to Data are trained in dealing with them.

Authorizations are granted only on the basis of valid username/password combinations or authentication keys explicitly created by the Controller for individual diagrams (for example, by "publish function" or by certificate). Only encrypted passwords are stored in the system (current hash algorithm + salt), so that no one - not even an employee of the Processor - can see a password in readable and otherwise usable form. At the request of the Controller, a single sign-on integration can also be activated.

The transfer of information from the data centers to third parties always requires the consent of the Processor, unless otherwise stipulated by mandatory law.

Backups are asymmetrically encrypted and stored in a different location based on current industry standards and secure key lengths. Access to it is very limited. The keys are kept physically separate.

Separation control

The software architecture of the SaaS solutions of the Processor follows a multi-tenant concept. Each customer receives on the system a work area completely separated from all other customers ("tenant"). This is technically reflected in a global authorization system for all repository objects and user data.

Each customer receives a self-contained space that only users authorized by the customer can access. At no time does the Processor access the Data in a workspace unless the Controller independently authorizes an employee of the Processor for a limited period of time as part of a support case.

All objects and artifacts stored in the Crismo repository are subject to a consistent authorization system. Access bypassing this authorization system is not possible for system-inherent reasons. This also applies to all server-side generated cache copies (for example, diagram preview graphics of various sizes provided for performance reasons). None of these objects can be accessed bypassing the authorization system.

The multi-tenant concept also applies accordingly, as long as the responsible person commissions and uses two or more work areas (tenants) for different purposes with the Processor.

The only way to bypass the authorization system would be direct access to the locally held database. This access is only possible for the main persons responsible (or their representatives) for the technical operation and maintenance of the productive systems. The persons responsible are obliged to refuse access to the Data, except for the purpose of system maintenance.

Pseudonymization (Art. 32 (1) lit. a DS-GVO; Art. 25 (1) GDPR)

Logging is done within the cloud environment for security and maintenance reasons. All user data is pseudonymized, unless the safety measures do not allow for it. An example is authentication monitoring, since here e-mail addresses are needed for the detection of attacks. Access to logs is earmarked and restricted to an explicitly authorized group of persons.

Personal data uploaded by the Controller in Crismo systems may need to be pseudonymised by the Controller.

2. Integrity (Art. 32 (1) lit. b GDPR)

Transfer control

The transfer of information from the data centers to third parties requires the consent of the Processor.

Access to the services of the Processor is generally only possible through a user-level login, without which no Data can be accessed. Access via API is also possible only through user-level login or a user-managed API key. The user login also applies to employees of the Processor and service technician. In order to prevent automated attacks, protective measures have been taken (e.g. Brute Force Protection).

Client-side access to the cloud systems is secured and encrypted according to industry standards and current algorithms (AES-256 bit and PFS or equivalent). The up-to-dateness and security of the algorithms and technologies used are regularly checked. When security problems are discovered or reported, the algorithms and technologies are changed. In no case, however, will there be a deterioration in level of security.

Administrative access is explained under "Administrative access control". It uses consistently encrypted connections according to industry standards and two-factor authentication.

If data is handed over to Crismo Customer Service by the responsible person on the Controller side, the Controller has to ensure that sufficient protection is used during transmission. Here, e.g. encrypted archives can be used and the password can be transmitted by phone. The Processor will provide a secure electronic handover location. It is explicitly recommended to encrypt with 256-bit AES or equal or higher. The transfer of physical media is not provided.

Entry control

There is an unavoidable, non-bypassable, application-side logging of the input, modify, and delete operations. The Controller can, upon request, have access to the generated protocol.

For technical reasons, a history log can only be assured for the last 12 months.

3. Availability and resilience (Art. 32 (1) lit. b GDPR)

Availability control

All Data is backed up at intervals of three hours (or less) on backup servers remotely located from the source servers. Before the data is transferred to the backup servers, an asynchronous encryption method based on current industry standards is used directly on the Data.

For decryption in case of disaster recovery, there is a separate private key required which is physically locked at more than one location.

In addition to the file encryption, a transfer to a locally distributed backup server also takes place via an encrypted line, with encryption based on current industry standards. All keys have a minimum length of 20 characters.

The servers generally use an antivirus/antimalware solution and rootkit protection.

To ensure data integrity and prevent loss, server systems generally use redundant RAID storage systems or equivalent.

The entire software development process, including troubleshooting, is subject to a quality assurance process that includes systematic testing. In particular, the automated tests should reveal whether new or modified components work within the expected parameters.

4. Regular review procedure

Assessing and evaluating (Art. 32 (1) lit. d DSGVO; Art. 25 (1) DSGVO)

The systems of the Processor are examined quarterly by vulnerability scanners and regularly subjected to external penetration tests. The results from this will be incorporated directly into the development process. Necessary adjustments will be made immediately.

Data centers used by the Processor are subject to periodic reviews to ensure their IT security.

Commission control

The Controller commissions the Processor exclusively with the hosting and operation of the product agreed upon in the Agreement. The Processor warrants that the Data will not be processed for purposes other than those specified in the Agreement.

The affected employees of the Processor or the Sub-Processors involved are instructed and obliged with regard to the purpose and instructions of the Controller.

Exceptions may need to be approved by the Controller.

Attachment 2 - „Existing Sub-Processors“

Sub-Processor	Service	Location / Data Centers	Legal Basis
Google Cloud EMEA Ltd / Google Ireland Ltd (Firebase / Google Cloud Platform)	Provision of server and storage infrastructure for the platform operation (Data Center Services)	EU (Belgium, Netherlands, Finland)	Google Cloud DPA + EU Standard Contractual Clauses
Mixpanel, Inc.	Product usage analysis (pseudonymous event/usage data); data ingestion via EU endpoint api-eu.mixpanel.com	EU endpoint (company headquartered in the USA)	EU Standard Contractual Clauses / EU-U.S. Data Privacy Framework

Note: The data centers used for the Processor’s SaaS solution are located within the EU (Belgium, Netherlands, Finland).

Attachment 3 - „Crismo AI (optional)“

(1) This Attachment applies solely to the optional AI feature “Crismo AI” (Claude integration) and only to the extent and for as long as the Controller actively uses this feature. If the Controller does not use this feature, this Attachment and the provisions below do not apply to it; in particular, the Sub-Processor named in this Attachment does not apply to the Controller.

(2) For the provision of the AI feature “Crismo AI”, the Processor engages the following Sub-Processor:

Sub-Processor	Service	Location / Data Centers	Legal Basis
Anthropic, PBC	Provision of the AI model functionality for the optional AI feature “Crismo AI” (processing of user inputs and outputs by Claude)	USA	EU Standard Contractual Clauses (Module 2/3, Implementing Decision (EU) 2021/914)

(3) The following measures apply in addition to Attachment 1 for processing carried out in connection with “Crismo AI”:

– Transmission security: Inputs and outputs are transmitted between the Crismo platform and Claude (Anthropic) exclusively via a TLS-encrypted connection in line with the state of the art.

– Data minimization: Only the data actually required for the specific Crismo AI feature used is transmitted to Claude; no further data is exported.

– Access control: Triggering Crismo AI features is subject to the same authorization and access controls as the rest of the Crismo platform pursuant to Attachment 1, Section A.2; only users authorized for this purpose can activate the feature.

– Retention at Anthropic: Inputs and outputs are retained by Anthropic in accordance with Anthropic's then-current standard retention period for the interface used, unless a zero-data-retention configuration has been agreed; the then-current period is set out in Anthropic's documentation.

– No training on customer data: Under Anthropic's applicable usage terms, data submitted via the API is not used by default to train Anthropic's own AI models. Upon request, a zero-data-retention configuration with correspondingly shortened retention periods can be agreed for the Controller.

– Handling of outputs: Outputs generated by Claude that the Controller stores within the Crismo platform (e.g. in a diagram or workflow) are, from that point on, treated as ordinary Data processed by the Processor and are subject to the general measures set out in Attachment 1.

(4) Any change to the Sub-Processor named in this Attachment shall be made in accordance with the requirements and procedures set out in § 7 of this DPA (prior notice, right to object, right of termination).