

**Crisp IM SAS**

crisp.chat

[dpo@crisp.chat](mailto:dpo@crisp.chat)

SIREN: 833085806

Address: 2 Boulevard de Launay, 44100 Nantes, France

## Parties

### Customer (the “Controller”)

Company Name: Ole Nepomuk MaiOffice Address: Goethestr. 70, 10625 BerlinCountry: GermanyRegistration NB: /Represented By: Ole Nepomuk Mai

### Provider (the “Processor”)

Company Name: **Crisp IM SAS**Office Address: **2 Boulevard de Launay, 44100 Nantes**Country: **France**Registration NB: **833085806**Represented By: **Baptiste Jamin**

Note that more GDPR resources are available at: <https://help.crisp.chat/en/article/nhv54c/>

# 1. Definitions

- “**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- “**Data Subject**” means the individual to whom Personal Data relates.
- “**Instruction**” means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).
- “**Personal Data**” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law
- “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
- “**Processing**” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.
- “**Processor**” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

## 2. Data Processing

1. The Processor shall process Personal Data for the Purpose as described in the Crisp Privacy Policy.

- Before or at the time of collecting personal information, the processor identifies the purposes for which information is being collected.
- The processor will collect and use of personal information solely with the objective of fulfilling compatible purposes, unless the Processor obtains the consent of the controller or as required by law.
- The Processor will only retain personal information as long as necessary for the fulfillment of those purposes.
- The processor can collect personal information by lawful and fair means and, where appropriate, with the knowledge or consent of the Controller.
- Personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.
- The processor shall protect personal information by reasonable security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.
- The Processor may only process the Personal Data on documented instructions from the Controller, including with regard to transfers to third countries or international organizations, unless required to do so by Union or member state law to which the Processor is subject (in such a case the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest).

2. The data is only hosted processed and hosted within a member of the European Union.

- Core infrastructure (Databases, Messaging Servers, APIs) is hosted in Amsterdam, Netherlands
- Plugin infrastructure (third party connectors) is hosted in Frankfurt, Germany
- The Processor's content delivery network contains servers outside the European Union. These servers are used as network relays to get endpoints closer from the Data Subject. Those network relays are not storing any customer data and European Data Subjects are in principle connected to a server hosted within a member of the European Union.
- The Processor's servers backups are hosted in Ireland only. Those backups are encrypted and redundant within the data center to prevent from any data loss.

3. Depending on how the Controller uses the service, the matter of Processing of personal data may cover the following types/categories of data:

- Email address (if provided by end-user, thus involving a consent)
- Phone number (if provided by end-user, thus involving a consent)
- Message exchanges
- Activity Status (online / offline)
- Activity Date and Time
- IP Address
- Device Type (operating system and browser)
- Geographic Location, City, Country (guessed from the IP address)
- Preferred language
- Timezone
- Website pages that were accessed
- Professional Life Data (Position, Employer, Business Address)
- Data guessed from public information on Google (Avatar, Twitter/Facebook handle)

4. The categories of Data Subjects whose Personal Data are Processed are as follows:

- Crisp operator users (ie. Crisp accounts)
- Crisp CRM contacts (ie. the end-users of Crisp users, stored in a team / website database)

### 3. Technical and organizational provisions

1. The Processor will, taking into account the nature of the Processing and insofar as this is reasonable possible, assist the Controller in ensuring compliance with the obligations pursuant to the GDPR to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These measures will guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, in view of the risks entailed by Personal Data Processing and the nature of the data to be protected. The Processor will in any case take measures to protect Personal Data against accidental or unlawful forgery, unauthorized distribution or access, or any other form of unlawful Processing.

- Two Factor Authentication on third-party services Crisp uses
- Our SSH keys are all password-protected
- All the features are designed around security and reliability
- Computers and servers running Crisp development tools are secured and up to date
- Crisp employees, agents, and providers are trained in data-security practices
- All our servers and services are running latest security updates and patched immediacy when a vulnerability is published
- All domains are protected using DNSSec
- Abusing IPs get automatically banned or rate limited (prevents brute-force attacks on accounts).
- We use strong encryption techniques on all public network channels (user messages, user data).

2. The Processor can't be held responsible when The Controller is using the software or processing data without following the technical guidelines or documentation provided by the Processor.

3. The Processor ensures that its personnel and contractors are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality.

4. The Controller can contribute or request audits and inspections but may not conduct an audit more than once per calendar year. The shall be proceeded by an independent company, which is not a competitor of the Processor or related. The Controller shall reimburse the Processor for any cost or expenses incurred as a result of the audit.

## 4. Data Breaches

1. In the event the Processor becomes aware of any incident that may have an impact on the protection of Personal Data, i) it will notify the Controller without undue delay and ii) will take all reasonable measures to prevent or limit (further) violation of the GDPR.
2. The Processor will, insofar as reasonable, provide all reasonable cooperation requested by the Controller in order for Controller to comply with its legal obligations relating to the identified incident.
3. The Processor will, insofar as reasonable, provide all reasonable cooperation requested by the Controller in order for Controller to comply with its legal obligations relating to the identified incident.
4. The Processor will, insofar as reasonable, assist the Controller with the Controller's notification obligation relating to the Personal Data to the Data Protection Authority and/or the data subject, as meant in Section 33(3) and 34(1) GDPR. Processor is never held to report a personal data breach with the Data Protection Authority and/or the data subject.
5. Processor will not be responsible and/or liable for the (timely and correctly) notification obligation to the relevant supervisor and/or data subjects, as meant in Section 33 and 34 GDPR.

## 5. Sub-Processors

1. The Processor is entitled to outsource the implementation of the Processing on the Controller's instructions to Sub-processors, either wholly or in part. The Processor will inform Controller of any intended changes concerning the addition or replacement of other processors.
2. The Controller reserves the right to object to any Sub-processor, provided that, in its opinion, Sub-processor data does not provide sufficient guarantees to implement appropriate technical and organizational data protection measures.
3. Processor obligates each Sub-processors to contractually comply with the confidentiality obligations, notification obligations and security measures relating to the Processing of Personal Data, which obligations and measures must at least comply with the provisions of this Processor's Agreement.
4. Sub-processing in the meaning of this agreement does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity, and resilience of the hardware and software of the data Processing equipment.
5. Where the controller, based upon the obligations under the GDPR, is obliged to provide information to a Data Subject about the Processing of his or her Personal Data, the Processor shall assist the Controller in making this information available. The Processor shall as soon as possible and in the most detailed manner possible, refer the requests (of complaints) of the Data Subject to the Controller and shall assist the Controller with any request from a Data Subject Requests concerning his or her rights under Applicable Legislation and in particular - but not only - his or her right of access, rectification, correction, objection, restriction of processing and the right to be forgotten the right of data portability. The Processor shall rectify, erase or process any other way when the Controller instructs so to enable the latter to comply with the request of the Data Subject.
6. The Controller agrees to the commissioning of the following sub-processor on the condition of a contractual agreement in accordance with applicable data protection laws:

Sub-Processor	Category	Purpose	Company Location	Data Location
DigitalOcean, LLC	Hosting	Main servers & data (ie. most data)	US	EU (NL + DE)
Vultr Holdings Corporation	Hosting	Email relay servers	US	no data held
Amazon Web Services, Inc.	Hosting	Encrypted backups storage	US	EU (IE)
Cloudflare, Inc.	Network	DNS, CDN & DDoS protection	US	no data held
Stripe Payments Europe, Ltd.	Payment	Credit-card processing	EU (IE)	US
PayPal (Europe) S.à r.l. & Cie, S.C.A	Payment	Payment processing	EU (LU)	no data held
Google, LLC	API Provider	Push notification delivery (via FCM)	US	no data held
Microsoft Corporation (Microsoft Azure)	API Provider	On-demand translation of messages	US	no data held

Notes and details on the above table:

1. All of our user data is stored within the European Union through our sub-processors, including backups, at the exception of their payment method details (eg. credit card), which are stored at a sub-processor within the United States.
2. We distinguish the sub-processor company location, with the final location in which actual data is being held (that is, Crisp user data). That is, to build clarity into where our sub-processor operators from, and where the servers hosting the actual data are located.
3. Whenever “no data held” is being mentioned, the aforementioned sub-processor is usually being used to pass data along over the network, without actually holding it on its permanent storage. Access logs may still be stored for a short duration (ie. less than a month), as to allow our network engineer investigate any technical issue, whenever relevant. Those logs are not used for any other purpose.
4. A DPA contract has been signed between our company and each of the listed sub-processors.
5. We chose to host all our user data in European Union countries that are known to be neutral regarding surveillance and Internet censorship, which are The Netherlands and Germany. Encrypted backups are stored in Ireland, as we require geographic cross-country redundancy of data for worst-case scenarios considerations.



## **6. Duration**

1. This agreement shall commence on the Commencement Date and shall continue in full force and effect until the termination of the Purpose.
2. The Controller will adequately inform the Processor about the (statutory) retention periods that apply to the Processing of Personal Data by the Processor.


## **7. Rectification, restitution and erasure of data**

1. The processor may not on its own authority rectify, erase or restrict the Processing of Personal Data that is being processed on behalf of the Controller (unless if this is required by law), but shall only do so on documented instructions from the Controller and in accordance to data retention rules associated to the Controller subscription plan. Upon expiry of the DPA, the Processor shall, at the choice of the Controller, return all the Personal Data transferred and the copies thereof to the Controller or shall delete and/or anonymize all the Personal Data in an irreversible manner and certify to the Controller that it has done so, unless the Applicable Legislation imposed upon the Processor prevents it from returning or destroying all or part of the Personal Data Processed.
2. If a Data Subject should apply directly to the Processor to the request the rectification, erasure, or restriction of his Personal Data, the Processor must forward this request to the Controller without delay.

## Annex 1 — Updates to this DPA

- **May 6, 2022:** OneSignal, Inc. has been replaced with Google, LLC as a sub-processor. The scope of this sub-processor is only limited to the necessary delivery of Push Notifications to all Crisp apps via FCM (Firebase Cloud Messaging). It is to be noted that Google, LLC was already a sub-processor of OneSignal, Inc., which previously provided third-party API access to FCM. This change effectively minimizes the flow of user data from Crisp to third-parties.

**SIGNED on behalf of the Controller**

Signature:   
Company: Ole Nepomuk Mai  
Name: Ole Nepomuk Mai  
Title: Business Owner (Inhaber)  
Date: 14.04.2023

**SIGNED on behalf of the Processor**

Signature:   
Company: Crisp IM SAS  
Name: Baptiste Jamin  
Title: CEO  
Date: May 6, 2022