KASAR SAS
KasarCRM

CONTRACTUAL DOCUMENT

Personal Data Processing Agreement (DPA)

VERSION	LAST UPDATED
2026-09-28	**2026-09-28**

Provider	KASAR SAS, share capital €1,000 · Paris RCS 999 602 865 · 60 rue François Ier, 75008 Paris
Contact	support@kasar.app

Contents

> This English version is provided for convenience only. In the event of any discrepancy, the French version prevails.

This Data Processing Agreement (the "**DPA**") forms an integral part of the agreement entered into between the Provider and the Customer (the "**Main Agreement**"), consisting of the KasarCRM **General Terms and Conditions** (`cgv.md`) and, for the Enterprise Plan, the **Enterprise Specific Terms** and the **Enterprise Order Form**. It governs the processing, by the Provider on behalf of the Customer, of the personal data contained in the Customer Data, in accordance with **Article 28 of Regulation (EU) 2016/679 ("GDPR")**.

1. Definitions

The terms "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "sub-processor" have the meaning given to them by the GDPR. Terms defined in the Main Agreement retain their meaning. In this DPA:

- **Controller**: the **Customer**, which determines the purposes and means of the processing of Customer Data.
- **Processor**: the **Provider (Kasar)**, which processes Customer Data on behalf of the Customer.
- **Sub-processor**: any third party engaged by the Provider to process data on behalf of the Customer (Appendix 3, Section A).
- **Personal Data**: the personal data included in the Customer Data (Appendix 1).

2. Roles and purpose

2.1. The Customer is the **controller**; the Provider is the **processor**. Where the Customer itself acts as processor for a third party, the Provider is a sub-processor, and the Customer warrants that it holds the necessary authorizations from its own controller.

2.2. The purpose of this DPA is to define the conditions under which the Provider processes Personal Data on behalf of the Customer in the course of providing the Service. The nature, purpose and duration of the processing, and the categories of data and data subjects, are described in **Appendix 1**.

2.3. The processing by the Provider of data for which **it is itself the controller** (accounts, billing, logs) is excluded from this DPA and described in the Privacy Policy. The Customer instructs the Provider to produce, from technical measurements of the use of the Service, the aggregated and anonymized statistics provided for in Article 12.3 of the General Terms; these statistics do not include any data relating to data subjects other than Users.

3. Term

The DPA applies throughout the term of the Main Agreement and for as long as the Provider processes Personal Data on behalf of the Customer. The confidentiality and return/deletion obligations survive its termination.

4. Documented instructions

4.1. The Provider processes Personal Data only on the basis of the Customer's **documented instructions**, **including with regard to transfers to a third country or an international organization**. Such instructions consist of: the Main Agreement, this DPA and its appendices, and the use of the Service through its features (configuration, queries, settings, activation of an integration or feature, automations configured by the Customer). Additional instructions are sent in writing to `support@kasar.app`; the Provider responds within a reasonable time and points out those that would exceed the scope of the Service or change its cost.

4.2. The Provider informs the Customer if, in its opinion, an instruction infringes the GDPR or another applicable provision.

4.3. The Provider processes data outside the instructions only where required to do so by Union or Member State law; in such case, it informs the Customer before the processing, unless prohibited by law.

4.4. **Exceeding instructions.** Should the Provider itself determine the purposes and means of a processing operation, it would be considered a controller in respect of that processing (Article 28(10) of the GDPR). The parties expressly exclude any intention to that effect: other than for the processing referred to in Article 2.3, the Provider acts solely as processor.

5. Confidentiality

The Provider ensures that persons authorized to process Personal Data, employees and contractors alike, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and receive the necessary training. This commitment survives the end of their employment or service contract.

6. Security of processing (Article 32 GDPR)

6.1. The Provider implements the appropriate technical and organizational measures described in **Appendix 2** to ensure a level of security appropriate to the risk. These measures may evolve to take account of the state of the art and of risks, **without reducing the overall level of security** during the term of the Main Agreement.

6.2. These measures include in particular: **logical isolation of data per Organization** (dedicated database schema per customer), **encryption at rest of communication content and of access secrets** for third-party services (AES-256-GCM), encryption in transit (TLS), access control and logging.

6.3. The Customer acknowledges that, in order to provide the **AI Features** and certain analysis and synchronization features, the relevant content is **decrypted** and then processed by the Provider and transmitted to the relevant sub-processors (see Article 11 and Appendix 3).

7. Assistance to the controller

7.1. **Data subject rights.** Taking into account the nature of the processing, the Provider assists the Customer, by appropriate technical and organizational measures (in particular the access, export, rectification and deletion features of the Service), in responding to requests to exercise data subject rights (Articles 15 to 22 GDPR). If a request is addressed directly to the Provider, the Provider forwards it to the Customer without responding to it itself, unless instructed otherwise.

7.2. **Security obligations and impact assessments.** The Provider assists the Customer in complying with its obligations under Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessment, prior consultation), taking into account the nature of the processing and the information available to it.

7.3. **Cost of assistance.** The following are included in the price of the Service: assistance provided through the features of the Service, assistance in the event of a data breach (Article 8) and cooperation with a supervisory authority that is incumbent on the Provider in its own right. Any other assistance exceeding normal use of the Service and what Article 28 of the GDPR reasonably requires (in particular custom extractions, responses to specific questionnaires or detailed contribution to an impact assessment beyond one (1) working day) is subject to a prior quote accepted by the Customer, established at the Provider's current daily rate. Nothing is due where the request arises from a breach by the Provider.

8. Personal data breach notification (Article 33 GDPR)

The Provider notifies the Customer of any Personal Data breach **without undue delay**, and where possible within **forty-eight (48) hours** after it has become reasonably certain that a breach affecting the Customer's Data has occurred, so as to enable the Customer to meet the deadline of Article 33 of the GDPR. Where the breach affects a sub-processor, this period runs from the time the Provider is informed by that sub-processor. The notification is sent by message to the Administrator's contact address and, where provided, to the Customer's security contact.

The notification describes, to the extent of the information available: the **nature** of the breach and, where possible, the categories and approximate number of data subjects and records concerned; the **likely consequences**; the **measures** taken or proposed to address it and mitigate its effects; the **contact details** of the Provider's point of contact. Where not all of this information is available within that period, the Provider sends an initial partial notification, then provides the missing information in phases, without undue delay.

The Provider does not make any notification to the supervisory authority or to data subjects on behalf of the Customer, unless instructed in writing by the Customer. Notification of a breach does not constitute an acknowledgement of fault or liability on the part of the Provider.

9. Sub-processors

9.1. **General authorization.** The Customer **authorizes** the Provider to engage the sub-processors listed in **Section A of Appendix 3** for the purposes of the Service.

9.2. **Safeguards.** The Provider imposes on each sub-processor, by contract, the data protection obligations provided for in Article 28(4) of the GDPR, offering a level of protection substantially equivalent to that of this DPA having regard to the nature of the service provided, in particular the obligation to provide sufficient guarantees to implement appropriate technical and organizational measures. Where the sub-processor offers only its standard terms, the Provider ensures that they include these obligations. The Provider remains liable to the Customer for the performance by these sub-processors of their obligations, under the conditions and within the limits of Article 14.

9.3. **Changes.** The Provider informs the Customer of any intended addition or replacement of a sub-processor at least **thirty (30) days** in advance, by any appropriate means (update of Appendix 3 and notification). The Customer may object, in writing and on objective grounds relating to data protection, within **fourteen (14)**

days. The Provider then endeavors to propose a solution, in particular the deactivation of the relevant feature for the Customer's Organization; if no solution is found within thirty (30) days of the objection, the Customer may terminate, without penalty, the part of the Service that uses the sub-processor concerned or, if it cannot be separated, the Subscription, with effect from the date on which that sub-processor is engaged. Only sums paid in advance for the terminated part and the unexpired period are refunded. An objection not based on objective grounds relating to data protection has no effect.

9.4. **Emergency.** In an emergency relating to security or to the failure of a sub-processor, the Provider may replace it without observing the period of Article 9.3; it informs the Customer without delay, and the Customer then has the right to object provided for in that article.

10. Location and transfers outside the European Union

10.1. **Location.** The primary hosting of Personal Data (database and file storage) is located in the **European Union** (Ireland); application functions run in the European Union (France). Certain processing is, however, carried out **outside the European Union**, in particular in the **United States**:

- the synchronization and asynchronous processing infrastructure (emails, LinkedIn and WhatsApp messages, imports, automations) and the meeting recording bot, operated on a **DigitalOcean** cluster located in **New York**;
- the routing of native telephony calls by **Twilio** (Article 10.4);
- certain AI Features (Article 11).

The list of the processing operations concerned, their location and the applicable transfer mechanism are set out in Appendix 3. **Migration of the DigitalOcean cluster to a European Union region is planned**; Appendix 3 will be updated once it takes effect.

10.2. **Transfer mechanisms.** Any transfer outside the EEA is governed by a mechanism compliant with Chapter V of the GDPR: an adequacy decision, including the **EU–U.S. Data Privacy Framework** ("**DPF**") for certified recipients, or the European Commission's **Standard Contractual Clauses** (Implementing Decision (EU) 2021/914). Where the Provider itself transfers data to a sub-processor established outside the EEA and not certified, it acts as **exporter** and enters into the applicable Standard Contractual Clauses (**Module 3**, processor to sub-processor). Where the Provider's contracting party is established in the Union and itself transfers the data outside the EEA, that transfer is governed by the safeguards put in place by that contracting party, as indicated in Appendix 3.

10.3. **Supplementary measures and transfer impact assessments.** The Provider implements the supplementary measures recommended by the EDPB (Recommendations 01/2020) where relevant: encryption in transit, minimization of the data transmitted, contractual non-retention commitments where available. The Provider prepares and keeps up to date an impact assessment for each transfer based on Standard Contractual Clauses for which it is the exporter. A summary is provided to the Customer upon written request, subject to confidentiality, within a reasonable time.

10.4. **Native telephony.** Native telephony calls ("kasar-voip") made from the application are routed and processed by **Twilio in the United States** (us1 region). Recordings are stored in the European Union (Appendix 3). This transfer is governed by Standard Contractual Clauses (Article 10.2).

10.5. **Requests from third-country authorities.** If the Provider receives from a public authority of a third country a request for access to Personal Data, it informs the Customer without delay, unless prohibited by law; it assesses the lawfulness of the request under Union law, challenges it where it appears manifestly unlawful,

discloses only the minimum required and documents the request. The Provider cannot be held liable for requests addressed directly to its sub-processors, which are bound in that respect by the safeguards referred to in Article 10.2.

11. Artificial intelligence

11.1. The AI Features use third-party AI model providers, acting as sub-processors (Appendix 3), to which the relevant content is transmitted in decrypted form. The providers, their functions and their processing locations are described in Article 13.2 of the General Terms and in Appendix 3.

11.2. **Model training.** In accordance with Article 13.3 of the General Terms:

- the Provider **does not use** Personal Data to train or improve artificial intelligence models;
- **Anthropic** is bound, under its contract with the Provider, not to use the transmitted content to train its models; **OpenAI** does not use it for that purpose according to the terms applicable to its application programming interface;
- **Deepgram** does not use it to train or improve its models, the Provider having excluded the transmitted content from its model improvement program.

11.3. **Retention by AI providers.**

- **Anthropic Ireland, Ltd**: the Provider has entered into a contractual **non-retention** ("zero retention") commitment: the transmitted content is processed to produce the output intended for the Customer and is then not retained by Anthropic, except where required by law or to combat use contrary to its usage policy; it is not used to train its models.
- **OpenAI**: according to OpenAI's documentation, abuse monitoring logs for the speech synthesis and speech transcription interfaces are retained for **thirty (30) days** by default.
- **Deepgram, Inc.**: Deepgram may temporarily retain the transmitted content, under the terms of its application programming interface, in particular for security purposes; it does not use it to train its models (Article 11.2).

11.4. **Automated decisions and the AI Act.** The Provider does not take any decision based solely on automated processing within the meaning of Article 22 of the GDPR. Automations, campaigns and actions of Léo are configured and triggered by the Customer, which is responsible for them (Articles 13.7 and 13.8 of the General Terms). The practices prohibited by Article 5 of Regulation (EU) 2024/1689 are prohibited.

12. Return and deletion of data at the end of processing

12.1. **Return.** At the end of the Main Agreement, the Customer has the retrieval period provided for in **Article 17.6 of the General Terms**, of at least **thirty (30) days**, to export its Personal Data in open and machine-readable formats, under the conditions of Articles 17.1 and 17.11 of the General Terms.

12.2. **Deletion.** Upon expiry of that period, the Provider **deletes** the Personal Data from its production environments and requests its deletion from its sub-processors under the conditions of their contracts, subject to backups (Article 12.3) and to statutory retention obligations; the Provider then informs the Customer, upon request, of the provision requiring such retention and the period concerned. The Customer may request early deletion in writing.

12.3. **Backups.** Residual copies contained in backups are not deleted individually: they are erased as the hosting provider's backup rotation cycle proceeds, the Provider's objective being their removal as soon as possible. Until erased, they remain protected by the measures of Appendix 2, are not subject to any active processing and are used only for restoration purposes (Article 15.6 of the General Terms). In the event of a restoration, the Provider re-applies the deletions made since the backup.

12.4. **Confirmation.** The Provider issues a **written confirmation of deletion** upon the Customer's request.

13. Audit

13.1. **Information.** The Provider makes available to the Customer the information necessary to demonstrate compliance with Article 28 of the GDPR: this DPA and its appendices, the record referred to in Article 13.5 and, upon request, the responses to a reasonable security questionnaire, once per twelve (12) month period.

13.2. **Documentary audit by default.** Any audit is first conducted on the basis of documents, using the information referred to in Article 13.1.

13.3. **On-site audit.** Where the Customer considers, following the documentary audit, that the information provided is not sufficient to demonstrate compliance with Article 28 of the GDPR, it may carry out an on-site audit, or have one carried out by an independent auditor who is not a Competitor of the Provider and who is bound by confidentiality, under the following conditions:

- at most **once per twelve (12) month period**;
- subject to at least **thirty (30) days'** prior written notice and an audit plan communicated at least fifteen (15) days in advance;
- during Business Hours (from 9h to 18h, Paris time, on Business Days), for a duration of no more than **two (2) Business Days**, without disrupting the Provider's operations or accessing data of other customers or the Provider's trade secrets, which are consulted on site, without copying;
- **at the Customer's expense**, the Customer bearing its own costs and those of its auditor as well as the time spent by the Provider, at the daily rate communicated before the audit;
- the audit report is provided free of charge to the Provider.

The audit covers the Provider and is conducted remotely as a priority. It does not extend to sub-processors, whose compliance is demonstrated by their certifications and audit reports (in particular SOC 2, ISO 27001), which the Provider communicates when it has them.

13.4. **Exceptions.** The notice period is reduced to **ten (10) Business Days**, and the frequency limit and the charging of the Provider's time do not apply, where the audit follows a **confirmed data breach** affecting the Customer's Data or a **request from a supervisory authority**. Where an audit establishes a breach by the Provider of its obligations under Article 28 of the GDPR, the Provider does not charge for its time and remedies the breach at its own expense in accordance with an agreed action plan; each party bears its other costs. The cost of remediation, which falls within the Provider's own obligations, is not counted against the cap referred to in Article 14.

13.5. **Record and point of contact.** The Provider maintains the record of categories of processing activities carried out on behalf of the Customer (Article 30(2) of the GDPR) and communicates it upon request. The Provider's point of contact for any data protection matter, including the reporting of security incidents and suspected breaches, is `support@kasar.app`.

14. Liability

14.1. The Provider's liability under this DPA, including in respect of personal data, is subject to the provisions of **Article 16 of the General Terms**, and in particular to the **single cap** in its Article 16.2: the sums actually paid by the Customer during the twelve (12) months preceding the event giving rise to liability, with a minimum of one hundred euros (€100), and never exceeding **fifty thousand euros (€50,000)**, whatever the Plan. This DPA establishes **no separate or increased cap**; sums due under the DPA and under the Main Agreement are counted against the same cap.

14.2. This cap does not apply in the event of gross negligence, wilful misconduct/fraud or personal injury (Article 16.3 of the General Terms). It governs relations between the parties, including recourse actions between them under Article 82(5) of the GDPR; it does not limit the rights that data subjects derive from Article 82 of the GDPR against each of the parties.

15. Relationship with the Main Agreement

15.1. With respect to matters governed by **Article 28 of the GDPR**, the provisions of this DPA apply in all circumstances and prevail over any conflicting provision of the Main Agreement (Article 2.3 of the General Terms). For all other matters, the order of precedence is that of Article 2.2 of the General Terms.

15.2. The governing law and jurisdiction are those of the Main Agreement.

Appendix 1: Description of the processing

Item	Description
Controller	The Customer (the Organization)
Processor	KASAR (KasarCRM), SAS, RCS Paris 999 602 865, 60 rue François Ier, 75008 Paris
Subject matter	Provision of a SaaS CRM service and its associated features
Nature of operations	Collection, recording, organization, structuring, storage, consultation, analysis (including by AI), synchronization, transmission, export, deletion
Purposes	Enabling the Customer to manage its customer relationships: contacts, companies, opportunities, communications (email, LinkedIn, WhatsApp, telephony), meetings, tasks, notes, dashboards
Duration	Term of the Main Agreement + return/deletion periods (Article 12)

Categories of data subjects (determined by the Customer):

- The Customer's contacts and correspondents (customers, prospects, partners);
- The Customer's Users and team members;
- Any person mentioned in synchronized communications or records.

Categories of Personal Data (determined by the Customer):

- Identification and contact data: last name, first name, email addresses, telephone numbers, postal address, LinkedIn URL, photo, job title;

- Content of **synchronized communications**: emails (subject, body, participants), LinkedIn and WhatsApp messages, telephone call metadata;
- **Recordings and transcriptions** of calls and meetings (if activated by the Customer);
- Relationship and commercial data: notes, tasks, status, source, interaction history, enrichment data, AI-generated summaries;
- Any other data that the Customer chooses to enter or import into free-text fields.

The Customer shall not import, enter or organize the collection of **special categories of data** (Article 9 GDPR), subject to their incidental presence, under the conditions of Article 11.4 of the General Terms.

Appendix 2: Technical and organizational security measures

- **Data isolation**: a dedicated PostgreSQL database schema per Organization, with logical isolation at the level of each transaction; strict validation of schema identifiers.
- **Encryption at rest**: AES-256-GCM encryption of communication content (message bodies) and of third-party secrets/credentials (OAuth tokens, sessions).
- **Encryption in transit**: TLS for communications between Users and the Service and with sub-processors; restrictive content security policy (CSP).
- **Access control**: User authentication, named accounts, management of roles and permissions by the Administrator.
- **Segregation of secrets**: payment card data never pass through the Provider (direct collection browser → payment provider); third-party access tokens are encrypted.
- **Logging and monitoring**: logging of operations on records, imports, integrations and logins; application monitoring.
- **Backups**: backups managed by the database hosting provider.
- **Sub-processing**: contractual commitments imposed on sub-processors (Article 9.2).

> This appendix describes the state of the measures as at the date of the last update; it may evolve, without reducing the overall level of security.

Appendix 3: Sub-processors and connected services

Last updated: 2026-09-28. Any change is notified under the conditions of Article 9.3.

A. Sub-processors of the Provider

They are involved for all Organizations, as soon as the relevant feature is used, without any further action by the Customer.

Sub-processor	Purpose	Processing location	Transfer outside the EEA and safeguards
Supabase	PostgreSQL database, file storage	Ireland (AWS `eu-west-1`)	Not applicable
Vercel	Application execution, monitoring	France (`cdg1` region)	Not applicable

Sub-processor	Purpose	Processing location	Transfer outside the EEA and safeguards
Upstash / Redis	Cache, processing queues, presence	Region stated in Upstash's terms	**Possible.** Standard Contractual Clauses (Upstash DPA)
Amazon Web Services (S3)	Storage of meeting and call recordings	Ireland (`eu-west-1`)	Not applicable
DigitalOcean, LLC	Cluster hosting the synchronization and processing workers (emails, LinkedIn and WhatsApp messages, imports, automations), the WhatsApp gateway and the meeting recording bot. Communication content and access sessions are processed on this cluster	**United States** (New York, `nyc1` region). Migration to a European Union region planned	**Yes.** Standard Contractual Clauses (Module 3) provided for by the DigitalOcean DPA
Anthropic Ireland, Ltd	AI models: text generation, analysis, summarization, Léo assistant, web search. Contractual non-retention commitment ("zero retention", Article 11.3); no training	Contracting party established in Ireland. According to Anthropic, inference may by default be routed to servers located in the United States, Europe, Asia or Australia	**Possible.** Transfers outside the EEA made by Anthropic under Standard Contractual Clauses (Anthropic DPA)
Deepgram, Inc.	Audio transcription of meetings, calls and voice memos. No training (Article 11.2); temporary retention under its API terms	United States	**Yes.** Standard Contractual Clauses (Module 3)
OpenAI	Speech synthesis of Léo's responses in the mobile application; fallback transcription (Whisper) when the primary transcription is unavailable. No training according to the API terms; abuse monitoring logs retained for 30 days	United States	**Yes.** Contracting party and safeguards according to the OpenAI DPA; transfers under Standard Contractual Clauses
Twilio	Native telephony "kasar-voip": call routing, numbers, recordings (Article 10.4)	United States (call routing); Ireland (storage of recordings)	**Yes.** Standard Contractual Clauses
Dropcontact	Search and verification of business email addresses, during enrichment and prospect search	France (EU)	Not applicable
Stripe	Payments and billing	EU / United States	Standard Contractual Clauses
Resend	Transactional emails (invitations, login links)	United States	Standard Contractual Clauses

B. Third-party services connected at the Customer's initiative

These services process data only if the Customer **connects the corresponding integration**, and only within the scope it authorizes. The Customer chooses them, maintains its own contractual relationship with each of them and accepts their terms: they act on behalf of the Customer, or as independent controllers, and **are not sub-processors of the Provider**. The Provider accesses them only to execute the integration, on the Customer's instructions; it is not liable for their processing, and Articles 9 and 10 do not apply to them. The

processing that the Provider itself carries out on data originating from these services does, however, fall under Section A (in particular DigitalOcean for synchronization). The list below is provided for information purposes; the location and safeguards of each service are governed by its own terms.

Service	Category	Data concerned
Google (Gmail, Calendar, Meet)	Messaging, calendar, transcripts	Emails, events, meeting transcripts
Microsoft 365 (Graph)	Messaging, calendar	Emails, events
LinkedIn	Messaging (connector under Article 10.6 of the General Terms)	LinkedIn messages and conversations of the connected account
WhatsApp	Messaging (connector under Article 10.6 of the General Terms)	WhatsApp messages of the connected account
Meta Lead Ads	Advertising	Leads from lead generation forms
Slack	Data connector	Messages from channels to which the Customer grants access
Notion, **Airtable**, **Google Sheets**	Data connectors	Content of connected databases and sheets
Customer's Supabase / PostgreSQL	Data source	Content of connected tables
Fathom, **Granola**	Meeting notes	Meeting recordings, transcriptions and notes
Aircall	Telephony	Calls, recordings and transcriptions
Applications connected by the Customer (API, MCP server, webhooks)	Article 10.8 of the General Terms	Data that the Customer chooses to transmit to them