PLANVORTEX

Article 28 GDPR

Data processing agreement

The agreement governing how we process, on your behalf, the personal data that passes through PlanVortex. It is here in full and downloadable as a PDF.

Version 1.0, of 4 September 2026.

You do not need to sign it or send it back

This agreement is incorporated by reference into the terms of use: it applies automatically between you and us from the moment you create an account, with no paperwork. Download it for your compliance file. If your organisation also needs a copy signed by both parties, write to us and we will send you one.

1. Parties and standing of this agreement

This agreement is entered into between TALIA SOFTWORKS, S.L., tax ID B05350616, registered with the Commercial Registry of Ciudad Real, Spain, owner and operator of the PlanVortex service (hereinafter, "the Processor" or "PlanVortex"), and the natural or legal person holding the PlanVortex customer account (hereinafter, "the Controller").

The Controller determines the purposes and means of the processing of the personal data it enters or manages through the service. The Processor processes such data solely on the Controller's behalf and in accordance with this agreement, pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR) and Spanish Organic Law 3/2018.

This agreement forms an integral part of the terms of use of the service and applies from the moment the Controller creates an account. In the event of any conflict between this agreement and the terms of use on data protection matters, this agreement prevails.

2. Subject matter, scope and duration

The subject matter of the processing is the provision of the PlanVortex service: connecting social media accounts, scheduling and publishing content, managing messages, comments and reviews, generating content with artificial intelligence where the Controller uses it, collecting statistics, and access to all of the above through the web interface and the public API.

The details of the processing — nature, purpose, types of personal data and categories of data subjects — are set out in Annex I, which forms part of this agreement.

The processing continues for the whole term of the contractual relationship between the parties and ends in accordance with clause 9.

3. Processing on documented instructions

The Processor shall process personal data only on documented instructions from the Controller, including with regard to international transfers. This agreement, the terms of use, the configuration the Controller sets in the service and the requests it makes through the interface or the API all constitute documented instructions.

The Processor shall not use the Controller's personal data for its own purposes. In particular, it shall not sell it, shall not disclose it to third parties for commercial or advertising purposes, shall not build profiles from it, and shall not use it to train artificial intelligence models, whether its own or third parties'.

If the Processor considers that an instruction infringes data protection law, it shall inform the Controller without delay and may suspend the execution of that instruction until the matter is clarified. Where Union or Member State law requires the Processor to process data beyond the instructions received, it shall inform the Controller before processing, unless that law prohibits such information on important grounds of public interest.

4. Confidentiality

The Processor shall keep the personal data processed confidential; this obligation survives the termination of the agreement.

The Processor warrants that persons authorised to process personal data have expressly undertaken to respect confidentiality or are under a statutory obligation of confidentiality, and that access is restricted to those who need it in order to provide the service.

5. Security of processing

The Processor implements the appropriate technical and organisational measures required by Article 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of data subjects. The measures in force are set out in Annex II.

The Processor may update the measures in Annex II provided that the resulting level of security is no lower than the one described. The measures are reviewed whenever the architecture of the service changes and, in any event, whenever a sub-processor is added.

6. Sub-processors

The Controller gives the Processor general authorisation to engage the sub-processors listed in Annex III for the provision of the service.

The Processor shall inform the Controller of any addition or replacement of a sub-processor at least thirty (30) days in advance, by email to the account administrators and by updating the public trust page. During that period the Controller may object on reasonable grounds relating to data protection; if the objection cannot be resolved, the Controller may terminate the agreement without penalty and with a refund of the unused pro-rata portion of the period already paid for.

The Processor shall impose on each sub-processor, by contract, data protection obligations equivalent to those in this agreement, and shall remain liable to the Controller for the sub-processor's failure to fulfil its obligations.

The social networks and other destination platforms to which the Controller chooses to connect its accounts are not sub-processors. When the Controller publishes content or manages messages on them, those platforms process the data as independent controllers, under their own terms and policies, and not on the Processor's behalf.

7. Assistance to the Controller

Taking into account the nature of the processing, the Processor shall assist the Controller, by appropriate technical and organisational measures and insofar as this is possible, in responding to requests to exercise the data subject rights of access, rectification, erasure, restriction, portability and objection.

The service allows the Controller to access, rectify, export and erase the personal data held in its account by itself, from the interface and from the API. Where that is not sufficient, the Processor shall provide such further reasonable assistance as is requested.

The Processor shall likewise assist the Controller in complying with the obligations under Articles 32 to 36 GDPR — security, breach notification, impact assessments and prior consultation — taking into account the nature of the processing and the information available to it.

8. Personal data breaches

The Processor shall notify the Controller without undue delay, and in any event within forty-eight (48) hours of becoming aware of it, of any personal data breach affecting data processed on the Controller's behalf.

The notification shall describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed to address it, and a point of contact. Where it is not possible to provide all the information at once, it shall be provided in phases without undue further delay.

9. Deletion or return of the data

On termination of the provision of the service, the Processor shall delete all personal data processed on the Controller's behalf, unless the Controller requests its return before closing the account. Data is exportable by the Controller itself, at any time and at no cost, through the public API.

Deletion is carried out by an automated process that runs daily and completes within a maximum of twenty-four (24) hours from the closing of the account. It covers the customer, its organisations, its connected accounts and credentials, its posts, statistics, conversations, comments, files and integrations.

Data whose retention is required by Union or Member State law is excepted, in particular billing documentation subject to accounting and tax rules, which is retained for the legally required periods with access limited to that purpose.

10. Information and audit

The Processor shall make available to the Controller the information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. Public documentation on security, data residency and sub-processors is permanently available on the trust page of the website, and the Processor shall additionally respond to reasonable security questionnaires sent by the Controller.

The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by it, upon request with at least thirty (30) days' notice, during business hours, without disrupting operations, at most once a year — save where required by a supervisory authority or following a demonstrated security breach — and subject to a confidentiality undertaking. The costs of the audit are borne by the Controller, unless breaches attributable to the Processor are found.

11. International transfers

Processing takes place within the European Economic Area, with the sole exception stated in Annex III. The Processor shall not transfer personal data outside the European Economic Area beyond what is set out in that annex without first informing the Controller in accordance with clause 6.

Any transfer to a third country not covered by an adequacy decision relies on the standard contractual clauses approved by the European Commission, supplemented by any additional measures found necessary following the corresponding assessment.

12. Liability

Each party is liable for the damage it causes by breaching the obligations imposed on it by this agreement and by the GDPR, on the terms of Article 82 GDPR.

The limitations of liability agreed in the terms of use also apply to this agreement, except where mandatory law does not permit such limitation.

13. Term, amendment and governing law

This agreement takes effect upon creation of the account and remains in force for as long as the Controller uses the service. The confidentiality and deletion obligations survive its termination.

The Processor may amend this agreement to adapt it to regulatory changes or to changes in the architecture of the service, giving at least thirty (30) days' notice. Each version is identified by its number and date, and previous versions are kept available to the Controller.

This agreement is governed by Spanish law and by the GDPR. For any dispute, the parties submit to the Spanish courts. The supervisory authority competent for the Processor is the Spanish Data Protection Agency (AEPD).

Annex I · Details of the processing

SUBJECT MATTER
Provision of the PlanVortex service for managing and publishing on social media, messaging, comments and reviews, AI content generation and statistics, through the web interface and the public API.

DURATION
For as long as the Controller's account is active, plus the twenty-four (24) hour deletion period described in clause 9.

NATURE
Collection, recording, structuring, storage, retrieval, alteration, disclosure by transmission to the destination platforms chosen by the Controller, and erasure.

PURPOSE
Solely to provide the Controller with the functionality it contracts and uses. The Processor has no purposes of its own.

TYPES OF PERSONAL DATA
Identification and contact data of the account's users (name, email address, language, role and permissions); billing data; identifiers, names and images of the connected social media profiles and their access permissions; the content of posts and of the files the Controller uploads; the content and identifiers of the conversations, comments and reviews the Controller manages, including the data of the people involved; and aggregate metrics of posts and profiles.

CATEGORIES OF DATA SUBJECTS
Users of the Controller's account; the Controller's own end customers where it manages third-party accounts; and people who interact with the connected profiles by writing messages, comments or reviews.

FREQUENCY
Continuous, for the duration of the contractual relationship.

Annex II · Technical and organisational measures

These are the measures actually implemented as at the date of this version.

- Encryption in transit. All traffic — website, dashboard and API — travels over HTTPS/TLS. There is no unencrypted route for communicating with the service.
- Isolation of access permissions. The OAuth tokens of connected accounts never leave the server: the API strips them from every response before issuing it, so they cannot be read from the interface, from an integration or from an activity log.
- Encryption of secrets at rest. API keys and application credentials supplied by the Controller are stored encrypted with AES-256-GCM on a write-only basis: they can be replaced, but never read back.
- Access control and authentication. Identity is managed with Keycloak; the Processor does not store passwords. Each API request carries an RS256-signed token that is verified server-side and checked against the specific permission the operation requires within the relevant organisation.
- Infrastructure isolation. Databases and cache are not exposed to the internet and are reachable only from the service itself. Staff access to production systems is limited to what is strictly necessary to operate them.
- Database redundancy. The database runs as a replica set, so the failure of a node neither interrupts the service nor causes the loss of acknowledged writes.
- File protection. Object storage is private, with no public or predictable addresses, and all access is through signed links that expire.
- Minimisation of third-party permissions. Each connected platform is asked for the minimum permission the feature in use requires, and it is revoked when the account is disconnected.
- Effective erasure. Closing an account triggers an automated full-deletion process completing within a maximum of twenty-four (24) hours, with no residual archiving.
-

Organisational measures. Authorised persons bound by a duty of confidentiality, access restricted to what is necessary, and review of the measures on every architectural change or addition of a sub-processor.

Annex III · Authorised sub-processors

The list in force as at the date of this version. Any addition or replacement is notified thirty (30) days in advance in accordance with clause 6.

IONOS SE
Spain (EU)
Hosting of the dedicated servers on which the service runs.

Cloudflare, Inc.
European Union (storage contracted under EU jurisdiction)
Storage of the files uploaded by the Controller (R2) and network and DNS protection.

Stripe Payments Europe, Ltd.
Ireland (EU)
Payment, subscription and invoicing processing. Card details are collected directly by Stripe and do not transit the Processor's systems.

OpenRouter, Inc.
United States (standard contractual clauses)
Routing of AI content generation requests to the model providers. It is involved only if the Controller uses the AI features, and receives solely the instructions entered and the content generated.

Google Ireland Limited
Ireland (EU), with possible transfers to the United States under the applicable adequacy framework
Audience measurement (Google Analytics 4), only with prior consent, and anti-fraud protection of the contact form (reCAPTCHA).

Data protection contact
For any question about this agreement, the exercise of rights or a security questionnaire: contact@planvortex.com.