DATA PROCESSING AGREEMENT

(GDPR Article 28)

between **TONVI TECH S.L.** ("Upload-Post" / Processor) and **THE CUSTOMER** ("Customer" / Controller)

Effective Date: as set out in Section 1.2 and the Terms of Use · Version 1.5 — 4 September 2026

1. Background and Parties

1.1 This Data Processing Agreement (the **"DPA"**) is entered into between:

TONVI TECH S.L., a Spanish limited liability company with Tax ID (C.I.F.) B-19780394 and registered office at Calle Puerta del Mar 18, 5th Floor, 29005 Málaga, Spain, trading as **"Upload-Post"** (hereinafter **"Upload-Post"** or the **"Processor"**); and

The legal entity that has accepted the Upload-Post Terms of Use or, where a copy of this DPA is executed bilaterally, the legal entity identified in the signature block (hereinafter the **"Customer"** or the **"Controller"**), acting on its own behalf and, where applicable, on behalf of its Authorised Affiliates.

Upload-Post and the Customer are individually referred to as a **"Party"** and collectively as the **"Parties"**.

1.2 This DPA forms an integral part of, and is governed by, the Upload-Post Terms of Use available at https://www.upload-post.com/terms-of-use and any related order form or subscription agreement (together, the **"Agreement"**). In the event of any conflict between this DPA and the Agreement regarding the Processing of Personal Data, this DPA shall prevail.

1.3 This DPA reflects the requirements of Regulation (EU) 2016/679 (the **"GDPR"**), the Spanish Organic Law 3/2018 (**"LOPDGDD"**), the UK GDPR where applicable, and any other applicable data protection laws (together, **"Data Protection Laws"**).

2. Definitions

Capitalised terms not defined in this DPA shall have the meaning given in the Agreement or in the GDPR. For the purposes of this DPA:

- **"Affiliate"** means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with, a Party.
- **"Connected Platform"** means any third-party social media platform or comparable service to which the Customer connects an account through the Services for the purpose of publishing content (including those listed in Annex III, Part B).
- **"Customer Data"** means any data, including Personal Data, submitted to, stored in, or processed through the Services by or on behalf of the Customer or its end users.
- **"Data Subject"**, **"Personal Data"**, **"Processing"**, **"Controller"**, **"Processor"** and **"Personal Data Breach"** shall have the meaning given in Article 4 of the GDPR.
- **"EEA"** means the European Economic Area.
- **"Material Amendment"** means a change to this DPA that materially reduces the protections afforded to the Customer's Personal Data, materially expands Upload-Post's permitted Processing activities, materially

modifies the Customer's rights of audit or objection, or imposes new material obligations on the Customer. Editorial corrections, clarifications, updates to reflect changes in applicable law or regulatory guidance, additions of new Sub-processors handled pursuant to Section 5, and updates to the technical and organisational measures that do not diminish the overall level of security are not Material Amendments.

- **"SCCs"** means the Standard Contractual Clauses for the transfer of Personal Data to third countries, approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended.
- **"Services"** means the social media publishing API, automation platform, and any related services provided by Upload-Post to the Customer under the Agreement.
- **"Sub-processor"** means any third party engaged by Upload-Post to process Personal Data on behalf of the Customer.
- **"Supervisory Authority"** means an independent public authority established by a Member State pursuant to Article 51 of the GDPR; in Spain, the Agencia Española de Protección de Datos (AEPD).

3. Scope, Roles and Processing Instructions

3.1 Roles of the Parties. The Customer is the Controller and Upload-Post is the Processor acting on behalf of the Customer. Where the Customer itself acts as a processor for a third-party controller, Upload-Post acts as Sub-processor and this DPA shall apply mutatis mutandis.

3.2 Subject Matter and Details of Processing. The subject matter, nature, purpose, duration of the Processing, the types of Personal Data and the categories of Data Subjects are described in Annex I to this DPA.

3.3 Documented Instructions. Upload-Post shall Process Personal Data only on the documented instructions of the Customer. The Agreement, this DPA and the Customer's lawful use of the Services constitute the Customer's complete and final documented instructions to Upload-Post. Any additional instructions require prior written agreement between the Parties.

3.4 Compliance with Laws. Upload-Post shall Process Personal Data in accordance with applicable Data Protection Laws. If Upload-Post believes that an instruction from the Customer infringes Data Protection Laws, Upload-Post shall immediately inform the Customer.

3.5 Controller Responsibilities. The Customer warrants and represents that: (a) it has provided all necessary notices and obtained all necessary consents and rights under Data Protection Laws for Upload-Post to lawfully Process Personal Data for the purposes contemplated by the Agreement; (b) its instructions to Upload-Post comply with Data Protection Laws; and (c) the Personal Data it submits to the Services does not infringe any third-party rights.

3.6 Role Allocation. The roles of the Parties depend on the category of data. Where a category is processed as Controller by Upload-Post, such Processing is governed by Upload-Post's Privacy Policy at https://www.upload-post.com/data-and-privacy-policy:

Data category	Upload-Post's role
Content submitted for publication (text, images, video, captions, media metadata)	Processor (on behalf of Customer)
OAuth tokens and credentials for Connected Platforms	Processor (on behalf of Customer)
Scheduling data, publication results, queues	Processor (on behalf of Customer)

Data category	Upload-Post's role
Service logs strictly necessary for service operation, security, abuse prevention and incident response	Processor (on behalf of Customer)
Account and billing data (Customer's contact, billing address, VAT ID, invoices)	Independent Controller
Product analytics, telemetry and aggregated usage metrics for service improvement	Independent Controller
Customer relationship and support communications initiated by Upload-Post	Independent Controller

4. Security Measures

4.1 Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing, as well as the risks to the rights and freedoms of natural persons, Upload-Post shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as set out in **Annex II** of this DPA.

4.2 Upload-Post shall ensure that any person authorised to Process Personal Data (including its employees and contractors) is subject to a duty of confidentiality of a statutory or contractual nature.

4.3 Upload-Post may update the security measures described in Annex II from time to time, provided that such updates do not materially diminish the overall level of security.

5. Sub-processors

5.1 General Authorisation. The Customer grants Upload-Post a general authorisation to engage Sub-processors for the performance of the Services, subject to the requirements of this Section 5. The current list of authorised Sub-processors is set out in **Annex III**.

5.2 Obligations of Sub-processors. Upload-Post shall enter into a written agreement with each Sub-processor containing data protection obligations no less protective than those in this DPA.

5.3 Changes to Sub-processors. Upload-Post shall provide notice of any intended addition or replacement of Sub-processors by updating the Sub-processor list published at https://www.upload-post.com/subprocessors or by email, at least thirty (30) days before the change takes effect. The Customer may object to the change on reasonable data protection grounds within fifteen (15) days of notice. If the Parties cannot agree on a resolution within a further thirty (30) days, the Customer may terminate the affected Services as its sole and exclusive remedy.

5.4 Liability for Sub-processors. Upload-Post shall remain fully liable to the Customer for the performance of each Sub-processor's obligations in accordance with the terms of this DPA.

6. International Data Transfers

6.1 EU-based Infrastructure. Upload-Post hosts and stores Personal Data primarily within the European Union. The hosting, object storage and product analytics Sub-processors are configured to operate within the EEA. The current data residency of each Sub-processor is set out in Annex III. The Customer acknowledges that some Sub-processors are part of group structures with parent or affiliated entities outside the EEA and may, in limited circumstances (such as administrative access, support, security operations or platform-level metadata), involve transfers covered by the safeguards described in Section 6.2.

6.2 Permitted Transfers Outside the EEA. Where, as part of the operation of the Services, Personal Data is transferred to a country outside the EEA that has not been the subject of an adequacy decision by the European Commission, such transfer shall be made pursuant to: (a) the SCCs, hereby incorporated by reference into this DPA; (b) the EU-U.S. Data Privacy Framework or its UK and Swiss extensions, where the recipient is certified; or (c) another transfer mechanism recognised under Article 46 GDPR. The applicable modules, the Parties' selections, and the details of the transfer are set out in **Annex IV**.

6.3 Connected Platforms. The Services involve, by their nature, the transmission of Personal Data to the Connected Platforms that the Customer chooses to connect. Upload-Post Processes such Personal Data as Processor for the limited purpose of transmitting the Customer's content to the Connected Platforms in accordance with the Customer's documented instructions. Once received by a Connected Platform, the Connected Platform Processes the data as an **independent controller** under its own terms of service, privacy notices and international data transfer mechanisms. Upload-Post has no control over how the Connected Platforms Process Personal Data thereafter.

6.4 Customer Responsibility for Connected Platforms. The Customer is responsible for: (a) selecting which Connected Platforms to use; (b) providing any notices to, and obtaining any consents from, Data Subjects required by Data Protection Laws for the transfer of Personal Data to such Connected Platforms; and (c) reviewing the privacy policies, terms of service and applicable transfer mechanisms of the Connected Platforms.

6.5 Transfer Impact Assessments. Where required by applicable Data Protection Laws, Upload-Post shall assess whether the laws and practices of the destination country may affect the effectiveness of the safeguards provided by the SCCs and shall implement appropriate supplementary measures (technical, organisational or contractual) where reasonably necessary. Upon the Customer's reasonable written request, Upload-Post shall provide information reasonably necessary for the Customer to perform its own transfer impact assessment, subject to confidentiality obligations.

6.6 Government Access Requests. If Upload-Post receives a legally binding request from a public authority for disclosure of Personal Data Processed on behalf of the Customer, Upload-Post shall: (a) where legally permitted, promptly notify the Customer of such request; (b) carefully review the legality and scope of the request and, where appropriate, challenge or seek to limit it; (c) provide only the minimum amount of Personal Data necessary to comply; and (d) maintain records of any such requests and responses for the Customer's review on reasonable request.

7. Data Subject Rights and DPIA Assistance

7.1 Assistance with Data Subject Requests. Taking into account the nature of the Processing, Upload-Post shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR.

7.2 Direct Requests. If Upload-Post receives a request directly from a Data Subject relating to Personal Data Processed on behalf of the Customer, Upload-Post shall, without undue delay, forward the request to the Customer and shall not respond to the Data Subject directly, unless authorised by the Customer or required by law.

7.3 DPIA and Prior Consultation. Upload-Post shall provide reasonable assistance to the Customer with any Data Protection Impact Assessments and any prior consultations with Supervisory Authorities, where the Customer reasonably considers such measures to be required under Articles 35 or 36 of the GDPR.

7.4 Fees. Upload-Post may charge a reasonable fee for assistance under this Section 7 that goes beyond standard features of the Services or that requires significant engineering effort, subject to prior written agreement with the Customer.

8. Special Categories of Personal Data

8.1 The Services are not designed or intended for the Processing of special categories of Personal Data within the meaning of Article 9 GDPR or data relating to criminal convictions and offences within the meaning of Article 10 GDPR (together, **"Sensitive Data"**).

8.2 The Customer shall not submit Sensitive Data to the Services unless: (a) the Processing is necessary for the Customer's legitimate operation of the Services; (b) the Customer has established a valid legal basis under Article 9(2) or 10 GDPR, as applicable; and (c) the Customer has notified Upload-Post in writing of the intended Processing.

8.3 The Customer acknowledges that content submitted to the Services may incidentally contain Sensitive Data of individuals appearing in images, video or text. The Customer is solely responsible for ensuring that any such Processing complies with Article 9 GDPR and for the data minimisation, retention and access controls applicable to such content.

9. Personal Data Breaches

9.1 Notification. Upload-Post shall notify the Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of the Customer. Upload-Post may provide an initial notification with the information then available and supplement it with further details as the investigation progresses.

9.2 Content of Notification. The notification shall, to the extent reasonably available at the time, include: (a) a description of the nature of the Personal Data Breach; (b) the likely consequences of the breach; (c) the measures taken or proposed to address the breach and mitigate its possible adverse effects; and (d) the contact details of a point of contact at Upload-Post.

9.3 Cooperation. Upload-Post shall cooperate with the Customer and take such reasonable steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9.4 No Admission. Notification of, or response to, a Personal Data Breach under this Section shall not constitute an admission of fault or liability by Upload-Post.

10. Audits and Information Rights

10.1 Upload-Post shall make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and this DPA.

10.2 The Customer may audit Upload-Post's compliance with this DPA once per calendar year, upon no less than thirty (30) days' prior written notice. The audit shall: (a) be conducted during normal business hours and on business days; (b) be subject to reasonable confidentiality obligations; (c) not unreasonably interfere with Upload-Post's business activities; (d) be limited to information and systems directly relevant to the Processing of the Customer's Personal Data; and (e) not exceed five (5) business days in aggregate duration per audit, unless otherwise agreed by the Parties in writing.

10.3 Additional Audits. The annual cap in Section 10.2 shall not apply where an additional audit is: (a) required by a Supervisory Authority or applicable Data Protection Law; or (b) reasonably necessary following a confirmed Personal Data Breach that materially affects the Customer's Personal Data. Such additional audits shall be conducted in good faith, with reasonable scope, on reasonable notice, and otherwise subject to the conditions in Section 10.2.

10.4 In the first instance, Upload-Post may satisfy its obligations under this Section 10 by providing relevant certifications, audit reports, security questionnaire responses, or other written documentation. On-site audits shall only be conducted where such documentation is reasonably insufficient and shall be conducted at the Customer's expense. Where the Customer engages a third-party auditor, that auditor must not be a competitor of Upload-Post and shall be subject to a written confidentiality agreement with Upload-Post.

10.5 Nothing in this Section shall require Upload-Post to disclose information that would compromise the security or confidentiality of other customers' data, trade secrets, or its own operational or commercial confidentiality.

11. Term, Return and Deletion of Personal Data

11.1 This DPA shall commence on the Effective Date and shall continue for as long as Upload-Post Processes Personal Data on behalf of the Customer under the Agreement.

11.2 Upon termination or expiry of the Agreement, at the Customer's choice, Upload-Post shall delete or return all Personal Data Processed on behalf of the Customer, and delete existing copies, unless Union or Member State law requires storage of the Personal Data.

11.3 The Customer may export its Personal Data at any time during the term of the Agreement using the functionality made available by the Services. If no choice is communicated by the Customer within thirty (30) days of termination, Upload-Post shall delete the Personal Data.

11.4 Upload-Post may retain Personal Data in back-up systems for a limited period consistent with its standard retention schedule (set out in Annex I, Part D), provided that such data remains subject to the confidentiality and security obligations set out in this DPA and is not further Processed.

12. Liability

12.1 Limitation of Liability. Subject to Sections 12.2 and 12.3, each Party's aggregate liability arising out of or in connection with this DPA, whether in contract, tort (including negligence), under statute or under any other theory of liability, shall not exceed the total fees paid by the Customer to Upload-Post under the Agreement during the twelve (12) months immediately preceding the event giving rise to the claim. This limitation applies in the aggregate to all claims and shall not be increased by reason of multiple claims arising from the same or related events.

12.2 Exclusions from the Cap. The limitation in Section 12.1 shall not apply to: (a) liability arising from a Party's fraud, gross negligence or wilful misconduct; (b) breach of a Party's confidentiality obligations; (c) indemnification obligations expressly set out in the Agreement; (d) liability for death or personal injury caused by negligence; and (e) any liability that cannot be excluded or limited under applicable law.

12.3 No Limitation on Data Subject Rights. Nothing in this DPA or the Agreement shall limit either Party's liability to Data Subjects under Article 82 GDPR, nor administrative fines imposed by a Supervisory Authority, nor any liability that cannot be limited by contract under applicable Data Protection Laws.

12.4 Exclusion of Indirect Damages. Subject to Section 12.2, neither Party shall be liable to the other for any indirect, incidental, special, consequential, exemplary or punitive damages, including loss of profits, revenue, business opportunity, or goodwill, arising out of or in connection with this DPA, even if advised of the possibility of such damages.

13. General Provisions

13.1 Governing Law and Jurisdiction. This DPA shall be governed by and construed in accordance with the laws of Spain. Any dispute arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the courts of Málaga, Spain, without prejudice to the rights of Data Subjects to bring proceedings before the competent Supervisory Authority or court under the GDPR.

13.2 Severability. If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

13.3 Amendments. Upload-Post may amend this DPA from time to time. Upload-Post will provide the Customer with at least thirty (30) days' prior written notice of any amendment, and the amendment will take effect at the end of that notice period.

Material Amendments (as defined in Section 2) shall require the Customer's prior written consent, which shall not be unreasonably withheld where the amendment is reasonably necessary to comply with applicable Data Protection Laws or guidance from Supervisory Authorities. If the Customer does not consent to a Material Amendment that is not strictly necessary for legal compliance, the Customer's sole and exclusive remedy shall be to terminate the affected Services without penalty.

Non-material updates (including, without limitation, additions of new Sub-processors in accordance with Section 5, clarifications, editorial corrections, and updates to the technical and organisational measures that do not diminish the overall level of security) shall take effect upon notice without requiring the Customer's consent, subject to the Customer's objection and termination rights set out elsewhere in this DPA where applicable.

13.4 Notices. Notices to Upload-Post under this DPA shall be sent to **info@upload-post.com**. Notices to the Customer shall be sent to the email address listed in the Customer's account or in the signature block of this DPA.

Signatures

The Parties have caused this DPA to be executed by their duly authorised representatives.

FOR UPLOAD-POST
TONVI TECH S.L.

Name: Victor Cavero Gracia

Title: Co-founder

Signature: 

Date: 21/09/2026

FOR THE CUSTOMER
Company: _____

Name: _____

Title: _____

Signature: _____

Date: _____

Annex I — Details of Processing

A. List of Parties

Role	Data Exporter (Controller)	Data Importer (Processor)
Name	The Customer, as identified in its Upload-Post account (or in the signature block of an executed copy)	TONVI TECH S.L.
Address	As identified in the Customer's account or signature block	Calle Puerta del Mar 18, 5th Floor, 29005 Málaga, Spain
Contact	As identified in the Customer's account or signature block	info@upload-post.com
Activities relevant to the transfer	Receiving the Services as described in the Agreement	Providing the Upload-Post social media publishing API and automation platform
Role under GDPR	Controller (or Processor, if acting on behalf of a third-party controller)	Processor (or Sub-processor, as applicable)

B. Description of the Processing

Subject matter of the Processing	Provision of the Upload-Post Services, including publishing and scheduling of content to Connected Platforms on behalf of the Customer, and optional AI-assisted content analysis and description generation.
Duration of the Processing	For the term of the Agreement and thereafter as set out in Section 11 of this DPA and the retention schedule in Part D below.
Nature and purpose of the Processing	The Processing consists of operations necessary to provide the Services, including: storing authentication tokens to Connected Platforms; receiving and temporarily storing content submitted by the Customer or its end users for publication; transmitting such content to the Connected Platforms via their APIs; storing publication results, scheduling data, service logs and security telemetry; where opted in by the Customer, processing short-form video content through third-party AI services to generate suggested titles and descriptions; sending transactional email (login, notifications) via Upload-Post's email provider; providing user management, billing, customer support and security monitoring.
Categories of Data Subjects	The Customer's authorised users who access the Services; the Customer's end users (where the Customer uses the Services on behalf of its own customers, e.g. white-label deployments); owners of the social media accounts connected to the Services; individuals identifiable in the content submitted to the Services.
Categories of Personal Data	Identification and contact data: name, email address, account identifier; authentication data: OAuth tokens and refresh tokens for Connected Platforms; Connected Platform metadata: handle, profile ID, profile information exposed by the platforms; content data: text, images, videos, captions, hashtags and any other data submitted for publication; usage and technical data: IP address, log data, device and browser information, API call metadata; billing data: billing contact, VAT ID, payment method metadata (full card details are processed by Stripe).
Special categories of data	See Section 8 of this DPA. The Services are not designed for the Processing of special categories of Personal Data or data relating to criminal convictions.
Frequency of transfer	Continuous, for the duration of the Agreement.

C. Competent Supervisory Authority

Agencia Española de Protección de Datos (AEPD), C/ Jorge Juan 6, 28001 Madrid, Spain — www.aepd.es

D. Retention Schedule

Upload-Post applies the following retention periods to Personal Data Processed on behalf of the Customer, subject to applicable legal requirements and the Customer's instructions:

Data category	Retention period
OAuth tokens and Connected Platform credentials	Until the Customer disconnects the relevant account, the token is revoked or expires, or termination of the Agreement, whichever occurs first.
Content pending publication	Until publication is completed or cancelled, plus up to 30 days for audit and troubleshooting purposes.
Published content references and publication metadata	For the duration of the Agreement, or as configured by the Customer through the Services.
Service logs (operational, performance)	Up to 90 days under standard configuration.
Security logs (access, authentication, anomaly detection)	Up to 12 months for security and incident response purposes.
Account and billing data	As required by applicable tax and commercial law (typically up to 6 years in Spain).
Back-ups	Up to 30 days from creation; back-ups are encrypted and read-only.
Aggregated or fully anonymised data	May be retained indefinitely; once anonymised, data no longer constitutes Personal Data.

Annex II — Technical and Organisational Measures

Upload-Post implements and maintains the following technical and organisational measures to protect the security of Personal Data. These measures are reviewed periodically and may be updated to reflect changes in the state of the art, provided that the overall level of security is not materially diminished.

1. Encryption

- All Personal Data in transit between the Customer and the Services is encrypted using TLS 1.2 or higher.
- Personal Data at rest is stored on encrypted file systems and/or in encrypted databases and object storage.
- Highly sensitive data, including OAuth tokens (see Section 2 below), is subject to additional field-level encryption with keys managed separately from the primary data store.

2. OAuth Token and Credential Security

Given the particular sensitivity of authentication credentials for Connected Platforms, Upload-Post applies the following additional measures to OAuth tokens, refresh tokens and equivalent credentials:

- Field-level symmetric encryption of tokens at rest (AES-128-CBC with HMAC-SHA256 authentication, Fernet specification), applied individually to each credential field.
- Encryption key stored outside the application database, in a protected environment variable of the runtime environment, with access restricted to authorised personnel.

- Strict least-privilege access: only the minimum set of services and personnel required to operate the Services may decrypt or use tokens.
- Use of the minimum OAuth scopes necessary to perform the publishing operations requested by the Customer.
- Centralised operational logging with automatic redaction of credentials and secrets prior to log persistence; token-related operations (refresh, use, authentication failures) are logged with request-level traceability for security and incident response purposes.
- Technical mechanisms for individual token revocation and account disconnection upon the Customer's request or following a security incident.
- In the event of a confirmed Personal Data Breach affecting the credential store, Upload-Post will initiate the encryption key rotation procedure without undue delay, and in any event within seventy-two (72) hours of confirmation of the incident.

3. Access Control

- Access to production systems is restricted to authorised personnel on a need-to-know basis.
- Administrative access requires individual user accounts, strong passwords, and multi-factor authentication (MFA).
- Access rights are reviewed periodically and revoked promptly upon termination of employment or change of role.
- All administrative access is logged for audit purposes.

4. Network and Infrastructure Security

- Production systems are hosted in secure data centres located within the European Union (Germany).
- Object storage is configured with the European Union jurisdictional restriction enabled where technically available. Limited administrative access, support, security operations or platform-level metadata may be processed by the Sub-processor's parent or affiliated entities, in which case the transfer is covered by the safeguards described in Section 6 of this DPA.
- Network traffic is filtered through firewalls and perimeter security controls.
- Systems are regularly patched and updated to address known security vulnerabilities.
- Security logs and alerts are monitored for anomalous activity.

5. Segregation and Isolation

- Customer data is logically segregated using per-account identifiers and access controls.
- Development, staging and production environments are separated. Where Personal Data is used in non-production environments for legitimate operational reasons (such as debugging), it is subject to the same security controls as production data and access is restricted to the minimum personnel required.

6. Backups and Business Continuity

- Regular automated back-ups of Personal Data are performed and securely stored within the European Union.
- Back-up data is encrypted.
- Recovery procedures are documented and periodically reviewed.

7. Personnel and Confidentiality

- All personnel with access to Personal Data are bound by written confidentiality obligations.
- Personnel receive data protection and security awareness guidance appropriate to their role.
- Access to Personal Data is limited to what is necessary to perform the person's duties.

8. Secure Software Development

- Code changes are subject to peer review before deployment to production.
- Dependencies are monitored for known security vulnerabilities.
- Authentication, authorisation and input validation are implemented in accordance with common industry best practices (e.g. OWASP guidelines).

9. Incident Response

- Upload-Post maintains a documented incident response procedure covering detection, containment, eradication, recovery and notification.
- Personal Data Breaches are notified to the Customer in accordance with Section 9 of this DPA.
- For incidents affecting OAuth tokens, the procedure includes invalidating affected credentials, initiating the encryption key rotation procedure within 72 hours of confirmation, requiring re-authentication for affected accounts, and coordinated notification to the Customer in accordance with Section 9 of this DPA.

10. Sub-processor Oversight

- Sub-processors are evaluated for their data protection and security practices before engagement, with a preference for providers established in or offering jurisdictional restrictions to the European Union.
- Sub-processor engagements are governed by written agreements incorporating data protection obligations no less protective than those in this DPA.

11. Physical Security

- Personal Data is stored in data centres with physical access controls (access cards, surveillance, 24/7 monitoring) operated by Upload-Post's hosting and storage Sub-processors.

12. Data Minimisation and Retention

- Personal Data is retained only for as long as necessary for the purposes of the Agreement or as required by law, in accordance with the retention schedule in Annex I, Part D.
- Deletion and anonymisation procedures are implemented at the end of the retention period.

Annex III — Authorised Sub-processors and Connected Platforms

A. Sub-processors

The following Sub-processors are authorised by the Customer pursuant to Section 5 of this DPA. This table, the list published at https://www.upload-post.com/subprocessors and the recipients section of our Privacy Policy are generated from the same source and are therefore identical. Last updated: September 4, 2026. Entries marked **self-hosted** run on infrastructure operated by Upload-Post itself (Hetzner, Germany); no third-party company receives the data.

Sub-processor	Location	Purpose	Transfer mechanism
Hetzner Online GmbH	Germany (EU)	Cloud hosting and infrastructure: application servers, MongoDB and Redis databases, back-up staging, GPU/staging server (balrog) and every self-hosted service listed below.	Intra-EEA; no third-country transfer.
Cloudflare, Inc.	European Union (R2 EU jurisdictional restriction) / United States (corporate access)	R2 object storage for media files uploaded for publication (media.upload-post.com and the scheduler bucket), plus CDN and DNS for our domains.	EU-U.S. Data Privacy Framework (Cloudflare, Inc. is certified) and EU Standard Contractual Clauses (Decision (EU) 2021/914) for any transfer outside the EEA.
Google Cloud EMEA Limited / Google LLC (Google Cloud Storage)	European Union (EU multi-region buckets) / United States (corporate access)	Encrypted-at-rest object storage for database back-ups, compressed server logs, copied profile pictures and scheduler payloads (buckets mongodb-img2html, logs-back, pfp-social-pics-upload-post-eu3, upload-post-schedulers-eu3).	EU-U.S. Data Privacy Framework (Google LLC is certified) and EU Standard Contractual Clauses, under the Google Cloud Data Processing Addendum.
Google LLC (Gemini API, paid tier)	United States	AI features: analysis of the full video you submit to the Shorts analyser (image and audio), generation of captions, titles, descriptions and hashtags, the support assistant and the documentation assistant.	EU-U.S. Data Privacy Framework and EU Standard Contractual Clauses. On the paid tier Google does not use the submitted content to train its models (Google APIs Terms of Service — Paid Services).
Google Ireland Limited / Google LLC (Google Ads)	Ireland (EU) / United States	Advertising measurement: the gtag conversion tag on the website (marketing cookies only, and only with your consent) and the Offline Conversions API, to which a SHA-256 hash of the buyer email address is sent when a subscription is paid.	EU-U.S. Data Privacy Framework and EU Standard Contractual Clauses, under the Google Ads Data Processing Terms.
Reddit, Inc.	United States	Advertising measurement for our Reddit campaigns: the Reddit advertising pixel (marketing cookies only, and only with your consent) and the Reddit Conversions API, to which a SHA-256 hash of the buyer email address is sent when a subscription is paid.	EU Standard Contractual Clauses (Decision (EU) 2021/914) and supplementary measures.
Stripe Payments Europe, Ltd. / Stripe, Inc.	Ireland (EU) / United States	Hosted checkout, subscription billing, invoicing, automatic VAT calculation and VAT-number collection. Card data is entered on Stripe pages and never reaches our servers.	EU-U.S. Data Privacy Framework and EU Standard Contractual Clauses.
Amazon Web Services EMEA SARL (Amazon SES)	France (eu-west-3)	Transactional email delivery: magic sign-in links, account and billing notifications.	Intra-EEA primary processing; EU Standard Contractual Clauses for incidental support access.
Namecheap, Inc. (PrivateEmail / Titan)	United States	Hosted mailbox for info@upload-post.com — receipt of customer correspondence and support requests — and fallback SMTP relay when Amazon SES is unavailable.	EU Standard Contractual Clauses.

Sub-processor	Location	Purpose	Transfer mechanism
Listmonk (self-hosted by TONVI TECH SL) Self-hosted	Germany (EU) — our own server at Hetzner	Newsletter and product-marketing email list (churnkiller.upload-post.com). Only subscribers who opted in receive marketing email; every message carries a one-click unsubscribe link.	Intra-EEA; no third-party processor involved.
OpenPanel (self-hosted by TONVI TECH SL) Self-hosted	Germany (EU) — our own server at Hetzner	Product and website analytics (api.openpanel.fotoexamen.com). The browser SDK is served from www.upload-post.com itself, so no third-party host sees your IP address. Analytics only runs with your consent.	Intra-EEA; no third-party processor involved.
Upload-Post media processing service "balrog" (self-hosted by TONVI TECH SL) Self-hosted	Germany (EU) — our own server at Hetzner	Server-side video processing with ffmpeg (trimming, re-encoding, subtitles, format conversion) for the media you submit. Processed results are deleted after 24 hours.	Intra-EEA; no third-party processor involved.
Upload-Post affiliate platform (self-hosted by TONVI TECH SL) Self-hosted	Germany (EU) — our own server at Hetzner	affiliates.upload-post.com — attribution of affiliate clicks and commissions. Receives the affiliate code, landing page, referrer and any advertising click identifiers, and later the conversion, plus the payout details of affiliates who join the programme.	Intra-EEA; no third-party processor involved.
Aikount — TONVI TECH SL Self-hosted	Spain (EU) — operated by the controller itself	Statutory invoicing and accounting for the invoices we are legally required to issue and keep (api.aikount.com). Receives the billing identifiers of the transaction (Stripe customer id, amounts, tax data).	Intra-EEA; same corporate group as the controller.
Telegram Messenger Inc.	Outside the EEA (United Arab Emirates / United Kingdom)	Internal operational and security alerts to the engineering channel (failed payments, sign-up abuse, platform restrictions). Being phased out; the alerts currently sent contain only pseudonymised identifiers (an 8-character hash plus the email domain) and a truncated IP address, never a full email address.	EU Standard Contractual Clauses are not available for this channel; the transfer is minimised to pseudonymised identifiers and the channel is being replaced by an internal alerting system.

B. Connected Platforms (Independent Controllers)

The following third-party social media platforms may act as recipients of Personal Data when the Customer connects them to the Services for the purpose of publishing content. Each of these platforms acts as an independent controller of the Personal Data it receives, as described in Section 6.3 of this DPA. This list is non-exhaustive and reflects the principal platforms supported by the Services as of the date of this DPA.

Platform	Operator	Transfer basis (as published by the operator)
Instagram, Facebook, Threads	Meta Platforms Ireland Ltd. (EU) / Meta Platforms, Inc. (US)	EU-U.S. Data Privacy Framework; SCCs.
TikTok	TikTok Information Technologies UK Ltd. / TikTok Technology Ltd. (Ireland)	SCCs and supplementary measures (Project Clover for EU data).

Platform	Operator	Transfer basis (as published by the operator)
YouTube	Google Ireland Ltd. / Google LLC (US)	EU-U.S. Data Privacy Framework; SCCs.
X (Twitter)	X Corp. (US)	SCCs.
LinkedIn	LinkedIn Ireland Unlimited Company / LinkedIn Corporation (US)	EU-U.S. Data Privacy Framework; SCCs.
Pinterest	Pinterest Europe Ltd. (Ireland) / Pinterest Inc. (US)	EU-U.S. Data Privacy Framework; SCCs.
Reddit	Reddit, Inc. (US)	SCCs.
Bluesky	Bluesky PBLLC (US)	SCCs.
Google Business Profile	Google Ireland Ltd. / Google LLC (US)	EU-U.S. Data Privacy Framework; SCCs.
Telegram, Discord, Slack, WordPress, Whop and other destinations you connect	The respective operator	As published by each operator.

The Customer is responsible for reviewing the privacy policies and terms of service of each Connected Platform and for ensuring that an appropriate legal basis exists for transferring Personal Data to such platforms. Upload-Post will use commercially reasonable efforts to keep this list up to date but does not warrant its completeness or accuracy at any given time, as the Connected Platforms' own arrangements may change.

Annex IV — Standard Contractual Clauses (SCCs)

1. Incorporation. Where the Processing under this DPA involves a transfer of Personal Data from the EEA, Switzerland or the United Kingdom to a country that has not been recognised as providing an adequate level of protection, the SCCs are hereby incorporated by reference and form an integral part of this DPA.

2. Applicable Module. The Parties select Module Two (Controller to Processor) where the Customer acts as Controller and Upload-Post acts as Processor. Where the Customer itself acts as Processor of a third-party controller, Module Three (Processor to Processor) applies.

3. Options and Selections. The Parties make the following selections under the SCCs:

- Clause 7 (Docking clause): does not apply.
- Clause 9 (Use of Sub-processors): Option 2 — general written authorisation, as set out in Section 5 of this DPA. Minimum notice period: thirty (30) days.
- Clause 11 (Redress): the optional language regarding independent dispute resolution does not apply.
- Clause 17 (Governing law): the SCCs shall be governed by the laws of Spain.
- Clause 18 (Choice of forum and jurisdiction): disputes shall be resolved before the courts of Málaga, Spain.

4. Annexes to the SCCs. Annex I to the SCCs (list of Parties, description of transfer, competent supervisory authority) is completed by reference to Annex I of this DPA. Annex II to the SCCs (technical and organisational measures) is completed by reference to Annex II of this DPA. Annex III to the SCCs (list of Sub-processors) is completed by reference to Annex III of this DPA.

5. UK Transfers. For transfers subject to the UK GDPR, the UK International Data Transfer Addendum issued by the UK Information Commissioner's Office applies in conjunction with the SCCs, with the tables of the Addendum populated by reference to the corresponding Annexes of this DPA.

6. Swiss Transfers. For transfers subject to the Swiss Federal Act on Data Protection, references in the SCCs to the GDPR shall be understood as references to the Swiss FADP where applicable, and the competent supervisory authority shall be the Federal Data Protection and Information Commissioner (FDPIC).

7. Conflict. In the event of any conflict between this DPA and the SCCs, the SCCs shall prevail with respect to the Processing of Personal Data transferred outside the EEA.
