LEGAL

Data processor agreement

Last updated: 23 July 2026

The undersigned

1. **Customer**, whose company and contact details and principal place of business are specified at the signature field below, hereinafter referred to as "**Controller**"

and

2. **Flipbase**, a private company with limited liability, incorporated and registered under the laws of the Netherlands having its registered office at the Zeestraat 61A, 2042 LB Zandvoort, registered with the Chamber of Commerce of the Netherlands under number 69080860, in this matter duly represented by Bram Tierie (Head of partnerships), hereinafter referred to as to as "**Processor**",

Processor and Controller are hereinafter also referred to individually as "**Party**" or collectively as "**Parties**".

Whereas

- The Processor shall provide, for the benefit of the Controller, an integrated, API-first video recording and playback technology. This technology standardizes the recording and playback processes, facilitating seamless integration into the Controller's software, thereby enabling the Controller to produce, manage, and publish video content efficiently.
- On signing date of this Processing Agreement document, the Controller and the Processor concluded an agreement regarding the provision of the aforementioned services, of which this Processor's Agreement is a part;
- Where the personal data processing is concerned, the Controller classifies as a controller within the meaning of Section 4(7) of the General Data Protection Regulation (*Algemene Verordening Gegevensbescherming*) ("GDPR");
- Where the personal data processing is concerned, the Processor qualifies as a processor within the meaning of Section 4(8) GDPR;
- The Parties, partly in implementation of the provisions of Section 28(3) GDPR, wish to document a number of conditions in the present processor's agreement which apply to their relationship in the context of the aforesaid activities on the instructions and for the benefit of the Controller.

Declare that they have agreed as follows:

Article 1. Definitions

1.1. In this Processor's Agreement, capitalized words and expressions, whether in single or plural, have the meaning specified as set out below:

Annex	appendix to this Processor's Agreement which forms an integral part of it;
Agreement	the agreement concluded between the Controller and the Processor with regarding the provision of services by Processor;
Personal Data	all information relating to an identified or identifiable natural person as referred to in Section 4(1) GDPR;
Process	as well as conjugations of this verb: the processing of Personal Data as referred to in Section 4(2) GDPR;
Processor's Agreement	the present agreement;
Sub Processor	the sub-contractor hired by Processor, that Processes Personal Data in the context of this Processor's Agreement on behalf of the Controller, as referred to in Section 28(4) GDPR;
Terms	the terms of use of Processor, which form an integral part of the Agreement.

1.2. The provisions of the Agreement apply in full to this Processor's Agreement. In case provisions with regard to the Processing of Personal Data are included in the Agreement, the provisions of this Processor's Agreement prevail.

Article 2. Purpose of the Personal Data Processing

2.1. The Controller and the Processor have concluded the present Processing Agreement for the Processing of Personal Data in the context of the Agreement. An overview of the type of Personal Data, categories of data subjects and the purposes of Processing, is included in **Annex 1**.

2.2. The Controller is responsible and liable for the processing of Personal Data in relation to the Agreement and guarantees that Processing is in compliance with all applicable legislation. Controller will indemnify and hold harmless Processor against any and all claims of third parties, those of the data protection authority in particular, resulting in any way from not complying with this guarantee.

2.3. The Processor undertakes to Process Personal Data only for the purpose of the activities referred to in this Processor's Agreement. The Processor guarantees that it will not use the Personal Data which it Processes in the context of this Processor's Agreement for its own or third-party purposes without the Controller's express written consent, unless a legal provision requires the Processor to do so. In such a case, the Processor shall immediately inform the Controller of that legal requirement before Processing, unless that law prohibits such information on import grounds of public interest.

Article 3. Technical and organizational provisions

3.1. The Processor will, taking into account the nature of the Processing and insofar as this is reasonably 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 destruction, accidental or deliberate loss, forgery, unauthorized distribution or access, or any other form of unlawful Processing.

3.2. The Processor will provide a document which describes the appropriate technical and organizational measures to be taken by the Processor. This document will be attached to this Processor's Agreement as **Annex 2**.

Article 4. Confidentiality

4.1. The Processor will require the employees that are involved in the execution of the Agreement to sign a confidentiality statement, whether or not included in the employment agreement with those employees, which in any case states that these employees must keep strict confidentiality regarding the Personal Data.

Article 5. Personal Data Processing outside Europe

5.1. The Processor will not transfer Personal Data outside the European Economic Area.

Article 6. Sub-processors

6.1. The Processor is entitled to outsource the implementation of the Processing on the Controller's instructions to Sub-processors, either wholly or in part, which parties are described in **Annex 3**. In case the Processor wishes to enable Sub-processors, the Processor will inform the Controller of any intended changes concerning the addition or replacement of other processors. The Controller will object to such changes within 5 working days. The Processor will respond to the objection within 5 working days.

6.2. 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.

Article 7. Liability

7.1. With regard to the liability and indemnification obligations of Processor under this Processor's Agreement the stipulation in Article 7 of the Terms regarding the limitation of liability applies.

7.2. Without prejudice to article 7.1 of this Processor's Agreement, Processor is solely liable for damages suffered by Controller and/or third party claims as a result of any Processing, in the event the specific obligations of Processor under the GDPR are not complied with or in case the Processor acted in violence of the legitimate instructions of the Controller.

Article 8. Personal Data Breach

8.1. In the event the Processor becomes aware of any incident that may have a (significant) 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.

8.2. 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.

8.3. 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.

8.4. Processors 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.

Article 9. Cooperation

9.1. The Processor will, insofar as reasonably possible, provide all reasonable cooperation to the Controller in fulfilling its obligation pursuant to the GDPR to respond to requests for exercising rights of data subjects, in particular the right of access (Section 15 GDPR), rectification (Section 16 GDPR), erasure (Section 17 GDPR), restriction (Section 18 GDPR), data portability (Section 20 GDPR) and the right to object (Section 21 and 22 GDPR). The Processor will forward a complaint or request from a data subject with regard to the Processing of Personal Data to the Controller as soon as possible, as the Controller is responsible for handling the request. The Processor is entitled to charge any costs associated with the cooperation with the Controller.

9.2. The Processor will, insofar as reasonably possible, provide all reasonable cooperation to the Controller in fulfilling its obligation pursuant to the GDPR to carry out a data protection impact assessment (Section 35 and 36 GDPR).

9.3. The Processor will provide the Controller with all the information reasonably necessary to demonstrate that the Processor fulfills its obligations under the GDPR. Furthermore, the Processor will, at the request of the Controller, enable and contribute to audits, including inspections by the Controller or an auditor that is authorized by the Controller. In case the Processor is of the opinion that an instruction relating to the provisions of this paragraph infringes the GDPR or other applicable data protection legislation, the Processor will inform the Controller immediately.

9.4. The Processor is entitled to charge any possible costs with the Controller.

Article 10. Termination and miscellaneous

10.1. With regard to the termination under this Processor's Agreement the specific provisions of the Agreement apply. Without prejudice to the specific provisions of the Agreement, the Processor will, at the first request of the Controller, delete or return all the Personal Data, and delete all existing copies, unless the Processor is legally required to store (part of) the Personal Data.

10.2. The Controller will adequately inform the Processor about the (statutory) retention periods that apply to the Processing of Personal Data by the Processor.

10.3. The obligations laid down in this Processor's Agreement which, by their nature, are designed to continue after termination will remain in force also after the termination of this Processor's Agreement.

10.4. The choice of law and competent court comply with the applicable provisions of the Agreement.

Annex 1. Overview personal data

Type of personal data

- video
- email address
- name
- related metadata, among others, but not limited to candidate or colleague identifiers, location, vacancy title, job title and department
- ip address

Categories of data subjects

In general the data subject is one or more individual(s) that can be identified in a video processed by the Processor. More specifically, in case Controller uses Processors Candidate Screening product the data subject is a candidate, who has applied or wants to apply at Controllers organization or organization the Controller mediates for. In case Controller uses Processors Employer Branding product the data subject is an individual that wants to help Controller to promote one or more vacancies, or the Controllers organization as a whole.

Purposes of processing

- To create multiple video formats available so users can playback them in all modern browsers
- To relate a submitted video with to an profile of an individual in an existing system, recruitment system or ERP system
- To be able to monitor and detect unauthorized attacks

Annex 2. Specification of the security measures

To shape information security according to multiple international standards we use the NEN-ISO/IEC 27001:2022 framework to create and evaluate the Security Management System. All information security implementations and measures are documented in the following documents:

- Risk assessment methodology

- Risk assessment
- Subcontractors document
- Privacy Impact Assessment
- Data Classification
- Security Policy
- Security Policy Summary
- Disaster recovery plan

Employees

This Security Policy document applies as a security agreement for employees of Processor. This document needs to be signed when employees start working at Processor. This document will be revisioned each year and therefore needs to be signed each year by all employees.

Processor employees are required to perform Processor related tasks on the provided devices, which have some pre-configured and pre-installed security measures. All devices are required to be password protected; hard disks need to be encrypted and firewalls need to be enabled.

Management

To make sure information security and business continuity is managed now and in the future, the Processors managing board commits to annual evaluations, updates and acts appropriately upon the information security management system and information security implementation.

This includes education and training of personnel, so they are able to handle sensitive information with care.

Password management

All passwords and credentials to third party systems and software need to be stored in a centralized password manager, which is accessible from the cloud. Employees of Processor are required to store all their passwords in 1Password manager. Additionally, specific password requirements apply, as defined in the security policy.

Suppliers & subcontractors

Every external information system or subcontractor Processor uses is documented in the ‘Subcontractors’ document. In case a supplier or subcontractor has access to personal identifiable or sensitive data, Processor makes sure a processing agreement is signed with the supplier or vendor which is in line with Processors default processing agreement.

Cryptographic management

We use only proven cryptographic algorithms with recommended key sizes, like AES and SHA 256. All cryptographic keys are only stored in a single, password encrypted file. No credentials or passwords are stored in source code.

Data at rest & data in transit

Data at rest, including video metadata and video content, are stored using AES 256 encryption. All data in transit is encrypted using the latest version TLS with a strong cipher suite.

Cookies

Cookies are encrypted to prevent malicious content to view cookies and/or modify it so that the confidentiality and integrity of the content of cookies is guaranteed. Cookie attributes are set to 'HttpOnly' and 'Secure' to prevent cookie information from being intercepted.

Development

We use source code versioning to manage the development process. Automated unit- & integration tests, static code analysis, linting tools and annual code reviews are used to maximize security.

Application security

The baseline of application security is based on OWASP implementation guidelines. All non-public REST API interfaces require an encrypted and validated customer bound signature to access or update a resource, so we can track 1) who is trying to access a resource and 2) can identify if this entity has the proper permissions to execute the specified action on the resource.

Monitoring

Servers are automatically and continuously monitored on, among others, but not limited to, CPU usage, memory usage, network activity and storage space. Applications are automatically and continuously monitored on, among others, but not limited to, request speed, request volume, errors and exceptions and crashes. If one metric exceeds a certain threshold an incident is triggered and reported automatically.

Logging

Processor uses a centralized log database where all log files and messages are sent to. This centralized system enables Processor to efficiently analyze any issue, anywhere in the whole architecture in real time and identify unexpected behavior.

Incident management

Any security incident can be reported by email by the Operations manager. Third parties can report incidents by sending an email to partners@flipbase.com. Reported incidents are classified and organized based upon the impact on the information security.

Disaster recovery

We have formalized a disaster recovery process that covers 1) a single data center (and all related availability zones) not being accessible, 2) a single availability zone in a single data center being done and 3) the related DNS servers being down.

Annex 3. Overview sub processors

- **Flipbase**

Flipbase utilizes multiple subcontractors to process personal identifiable data. However, we try to limit the number of subcontractors that process this personal identifiable data to a minimum. The companies listed below process personal identifiable data.

Subcontractor	Which data is being processed?	In which countries is data being processed?	Does the processor store the processed data?
Amazon Web Services	Hosting; transcoding submitted video files into multiple formats that are compatible for the web; processing and storing video metadata; storage of encoded video files; scanning content of video files on malicious content; serving video files to web clients	Frankfurt, Germany and Dublin, Ireland	Yes, but only in accordance with retention periods agreed upon the Controller
Google Cloud	Encrypted backups of video files and video metadata	European Union	Yes, but only in accordance with retention periods agreed upon the Controller
TransIp	Acting as a domain name server provider, the processing all web requests	Amsterdam, the Netherlands	No
MongoDB Cloud Atlas	Processing and storing video metadata	Frankfurt, Germany	Yes, but only in accordance with retention periods agreed upon the Controller