Biometric Addendum to the DPA — Sport Module

Version v3.0

En vigueur depuis le 30 octobre 2026

Publié le 30 octobre 2026

Langue : EN

Version 3.0 — October 30, 2026
Sport Module — Facial Recognition — Article 9 of the GDPR

Preamble

This addendum (hereinafter "the Addendum") supplements the Data Processing Agreement (hereinafter "the DPA") concluded between Attimo (Processor) and the photographer subscribed to the Platform (Data Controller, hereinafter "the Client").

It exclusively concerns the processing of biometric data implemented within the framework of the Attimo Platform's Sport module, which falls under the special categories of data within the meaning of Article 9 of the GDPR.

This Addendum applies only when the Sport module is activated on the Client's account and the Client uses facial recognition features. It is accepted by the Client upon first use of the module by means of a separate checkbox.

> ⚠ **IMPORTANT — Biometric data is sensitive data within the meaning of Article 9 of the GDPR.** Its processing is strictly regulated and requires reinforced safeguards. The Client is responsible for collecting the explicit consent of the persons concerned.

> **i GDPR Standards Applied to All Users**
>
> Regardless of the user's country of residence, Attimo applies European GDPR standards as the highest benchmark for biometric data protection. Users located outside the European Union benefit from these standards by contractual extension, in addition to any mandatory rights granted by their local jurisdiction (such as BIPA in Illinois, biometric provisions of the CCPA in California, or PIPEDA in Canada).

> **ℹ Changes introduced in version 3.0.** This version describes the facial recognition of the players of a sports club: the template of each authorised player's identity photo, and the analysis of the match photos in a team's batch to be sorted, whose face templates and read jersey numbers are retained for a maximum of thirty (30) days (Article 6.4).

Article 1 — Purpose of the Addendum

The purpose of the Addendum is to define the specific conditions under which Attimo processes, on behalf of the Client, biometric data of persons appearing in photographs uploaded within the framework of the Sport module.

This processing aims to allow end clients (athletes, spectators) to easily find the photographs in which they appear, by means of:

- Optical Character Recognition (OCR) on bib numbers.
- Facial recognition (selfie-search) for athletes wishing to find their photos by sending a selfie.
- For a sports club, facial recognition of the players in match photos, based on their identity photo, in order to offer the Client to file each photo in the gallery of the authorised players who appear in it.

Article 2 — Nature and Purpose of Biometric Processing

2.1 Data processed

The biometric data processed within the framework of the Sport module is as follows:

- Facial biometric templates extracted from photographs by the Amazon Rekognition service (mathematical vectors representing facial characteristics).
- Facial biometric templates extracted from selfies submitted by athletes for search.
- For a sports club: facial biometric templates extracted from the identity photo of each player of the team.
- For a sports club: facial biometric templates of all persons visible in the match photos placed in a team's batch to be sorted (players, opponents, spectators), together with the position of each face in the image.
- Associated metadata (similarity scores, timestamp, technical identifiers).

Attimo neither retains nor stores the original photographs of submitted selfies: these images are processed in random access memory only, sent to AWS Rekognition for analysis, then

immediately deleted. No selfie is ever written to disk.

For a sports club, each photograph in the batch to be sorted is analysed only once: the templates of the faces it shows and the jersey numbers read in it (the latter are not biometric data) are retained for the duration of the sorting, within the limits of Article 6.4, in order to search for players added later without analysing the same photographs again. Only the active players of the team whose authorisation is signed are searched for: the face of a person who has not given their consent is never attributed to anyone. No photograph is filed in a player's gallery without the Client's validation.

2.2 Purposes

Biometric processing has the sole purpose of facilitating photograph searches by data subjects and, for a sports club, filing match photographs in the gallery of the authorised players. They are not used for any other purpose, in particular:

- No commercial or advertising purpose.
- No transmission to third parties for profiling purposes.
- No use for police, administrative or judicial identification.
- No training of artificial intelligence models.

Article 3 — Legal Basis of Processing

In accordance with Article 9, paragraph 2, point a) of the GDPR, the processing of biometric data requires the **explicit consent** of the data subject.

The Client undertakes to collect, for each biometric processing, the explicit, free, specific, informed and unambiguous consent of each data subject, by means of:

- Clear and visible information at the sports event site (display panel, mention on the organizer's website, mention in the event regulations).
- An unchecked checkbox at the time of registration for the event or when accessing the photo gallery.
- A simple and effective possibility to withdraw consent at any time (opt-out).

For a sports club, consent is collected through the authorisation signed online by the adult player or by the holder of parental authority. The default authorisation text provided by the Platform informs the person of the facial recognition, of the retention period and of the effect of withdrawing their consent. Where the Client writes its own authorisation text, it is the Client's responsibility to include this information.

> **i Attimo provides the Client with templates of texts** (event panel, website

mention, checkbox paragraph, opt-out form) for indicative purposes only, to facilitate compliance. These templates do not constitute legal advice and do not replace validation by a legal professional. The use of these templates is the sole responsibility of the Client, who remains solely responsible for the effective and compliant collection of the consent of data subjects.

Article 4 — Subsequent Processor: Amazon Web Services

4.1 Use of AWS Rekognition

For the implementation of facial recognition features, Attimo uses the Amazon Rekognition service, provided by Amazon Web Services EMEA SARL.

Provider: Amazon Web Services EMEA SARL
Service: Amazon Rekognition (image analysis and facial recognition)
Processing location: Europe region — Ireland (eu-west-1)
Website: https://aws.amazon.com

4.2 Safeguards

Processing performed by AWS Rekognition within the framework of the Sport module is configured according to the following parameters:

- Processing exclusively carried out in the European region eu-west-1 (Ireland).
- No data transfer to the United States or outside the European Union.
- Explicit activation of the option of non-use of data for the improvement of AWS services.
- Encryption of data in transit (TLS).
- Encryption of data at rest by AWS (AES-256) in accordance with AWS standards.
- Automatic deletion of biometric collections at the end of the planned retention period.

i AWS acts as a subsequent processor within the meaning of Article 28 of the GDPR. The contract between Attimo and AWS includes the standard contractual clauses adopted by the European Commission, guaranteeing a level of protection equivalent to that of the GDPR.

Article 5 — Specific Obligations of Attimo

Within the framework of this Addendum, Attimo undertakes to:

1. Carry out biometric processing exclusively on infrastructures located in the European Union (AWS Ireland region).
2. Not use biometric data for purposes other than those provided for in this Addendum.
3. Implement the reinforced technical measures provided for in Article 7.
4. Allow any data subject to exercise their right to erasure under the conditions provided for in Article 8.
5. Automatically delete biometric collections at the end of the retention period provided for in Article 6.
6. Not carry out training of artificial intelligence models on biometric data.
7. Provide the Client, upon request, with the technical information necessary to carry out a Data Protection Impact Assessment (DPIA) as provided for in Article 9.

Article 6 — Retention Period

The retention periods of biometric data are strictly limited to what is necessary for the purpose of the processing.

6.1 Athletes' biometric templates

Biometric templates generated from uploaded photographs are retained for the lifetime of the corresponding sports gallery, fixed by the Client.

In accordance with Attimo's gallery lifecycle policy, this duration is contractually capped at twelve (12) months maximum per lifecycle, followed by a grace period of thirty (30) days.

At the end of this period, two scenarios are possible:

- Paid renewal of the gallery (extension of 12 additional months via payment): the templates are retained for the new period.
- No renewal: biometric templates are automatically and irreversibly deleted, at the same time as the corresponding gallery.

6.2 Biometric templates of selfies submitted for search

Biometric templates generated from selfies sent by athletes for search are processed in random access memory and deleted immediately after processing the request. They are not subject to any persistent storage.

6.3 Original photographs

Original photographs remain subject to the gallery lifecycle defined by the Client. Their retention or deletion is independent of the biometric processing.

6.4 Sports club: identity photo and match photos

By way of derogation from Article 6.1, for a sports club:

- The biometric template of a player's identity photo is retained for as long as the player is part of the team. It is deleted when the authorisation is refused, when the identity photo is changed or removed, when the player is removed from the team and when the team is deleted.
- The biometric templates of the faces visible in the match photos of a team's batch to be sorted, the position of these faces and the jersey numbers read are retained for a **maximum of thirty (30) days** from the first analysis of the batch.

These match photo templates, positions and numbers are deleted:

- immediately, when the Client empties the batch to be sorted;
- at the latest the following night, for a photograph transferred to the galleries or removed from the batch;
- together with the team, when it is deleted;
- in any event, at the latest thirty (30) days after the first analysis of the batch, by the Platform's automatic daily processing.

The faces of persons who have not given their consent (opponents, spectators, players whose authorisation is not signed) are never attributed to anyone and are deleted together with the others. After each deletion, the Platform checks with AWS that the templates have disappeared; any remaining template is deleted at the next run and the incident is reported to Attimo's administrator.

> ℹ **The deletion of biometric templates** (upon gallery expiration or upon erasure request) does not entail the deletion of the photographs themselves. The photographs remain accessible in the gallery as long as it remains active, but search by facial recognition is no longer possible once the templates are deleted.

Article 7 — Reinforced Security Measures

Given the sensitive nature of biometric data, Attimo implements reinforced security measures:

7.1 Technical measures

- Encryption of biometric data in transit via TLS on all communications (browser → Attimo → AWS).

- Encryption of data at rest provided by AWS (AES-256) in accordance with AWS standards for the Rekognition service.
- Strict isolation of biometric collections by event and by Client: each sports event has its own AWS collection named uniquely (technical format "attimo_event_{id}"). No crossover is possible between events or between Clients. For a sports club, each team has its own collection (technical format "attimo_roster_{id}"): the players of a team are searched for only in the photos of that team.
- Selfie processing in random access memory only: files are never written to the Attimo server's disk. The browser → RAM → AWS → deletion cycle is executed without persistence.
- Restriction of access to AWS Rekognition APIs to only the necessary automated processes. No direct human access to biometric templates.
- Exhaustive logging of all calls to AWS APIs via the dedicated service (logUsage).
- Use of dedicated AWS access keys (IAM user attimo-rekognition) with permissions strictly limited to the Rekognition service.
- Implementation of high confidence thresholds to limit false positives: minimum threshold of 93% for AWS facial recognition (FaceMatchThreshold), configurable per tenant.

7.2 Organizational measures

- Access to biometric data strictly limited to automated technical functions of the Platform.
- No visualization or manual manipulation of biometric templates by any person whatsoever.
- Documented procedure for managing security incidents specific to biometric data.

Article 8 — Right to Erasure (Opt-Out)

Any data subject has a right to erasure of their biometric data, which is exercised as follows:

8.1 Direct request to Attimo

The data subject can send their request directly to Attimo by email at: info@attimo-gallery.com. Attimo proceeds to delete all corresponding biometric templates within a maximum period of 72 hours from the receipt of the verified request.

8.2 Request via the Client (photographer)

The data subject may also send their request to the Client (photographer), who transmits it to Attimo for execution. The Client undertakes to transmit the request without delay.

8.3 Confirmation

Attimo confirms the deletion by email to the data subject (or to the Client if the request transited through them).

> ℹ **The deletion of biometric templates does not automatically entail the deletion of the photographs in which the person appears.** The person may separately request the deletion of the photographs directly from the photographer (Client), data controller for this data.

Article 9 — Data Protection Impact Assessment (DPIA)

The systematic and large-scale processing of biometric data may constitute high-risk processing within the meaning of Article 35 of the GDPR, requiring the carrying out of a Data Protection Impact Assessment (DPIA).

The Client is responsible for assessing the necessity of a DPIA given the scale and specificities of their activity. This assessment depends in particular on the number of events photographed, the number of persons concerned and the nature of the public (minors, professional athletes, general public, etc.).

Upon request from the Client, Attimo makes available the technical information necessary for carrying out this DPIA, provided in the form of a standard technical fact sheet including:

- Detailed technical description of biometric processing (processing pipeline, data flows, durations).
- Technical and organizational security measures implemented by Attimo (as described in Article 7).
- Retention periods applied (as described in Article 6).
- List of subsequent processors involved and their location (as described in Article 4).
- Description of the GDPR responsibility chain.

This technical fact sheet is sent to the Client by email upon simple request addressed to info@attimo-gallery.com.

Article 10 — Specific Obligations of the Client

Within the framework of this Addendum, the Client undertakes to:

1. Collect the explicit consent of the data subjects prior to any biometric processing, in accordance with Article 3.

2. Implement sufficient information measures (panels at the event site, mentions on websites, etc.).
3. Allow data subjects to easily exercise their right to erasure (opt-out).
4. For a sports club, where a player or their legal representative withdraws consent, remove the player from the team or remove their identity photo in the Platform without delay, which entails the deletion of their biometric template.
5. Not activate facial recognition for events predominantly involving minors without explicit parental authorization.
6. Carry out, where applicable, a Data Protection Impact Assessment (DPIA) before large-scale deployment.
7. Maintain a record of processing activities in accordance with Article 30 of the GDPR.
8. Notify Attimo of any request for the exercise of rights or any complaint received directly from data subjects.

Article 11 — Breach Notification

In case of a breach specifically concerning biometric data, Attimo notifies the Client within a maximum of 24 hours (instead of 48 hours provided for in the main DPA), given the sensitive nature of this data.

The notification includes a precise assessment of the potential impact on data subjects and emergency measures taken.

Article 12 — Liability

Each Party remains responsible for compliance with their respective obligations provided for in this Addendum and by the GDPR.

The Client acknowledges that they are solely responsible for collecting the explicit consent of data subjects and for the compliance of their activity with the legal obligations applicable to the processing of biometric data.

In case of a sanction pronounced against a Party following a failure of the other Party to comply with the obligations of this Addendum, the defaulting Party may be required to indemnify the other under the conditions provided for in the main DPA.

Article 13 — Term and Termination

This Addendum enters into force upon first use of the Sport module's facial recognition features by the Client and remains in force as long as the Client uses these features.

The activation and deactivation of the Sport module on the Client's account fall under Attimo's sole competence, based on the subscription plan subscribed by the Client and on administrative decisions made by Attimo (deactivation of a specific module via the Attimo administration interface).

In case of deactivation of the Sport module on the Client's account, for whatever reason (plan change, decision by Attimo, termination of the Main Contract), the following effects apply:

- Immediate cessation of any new biometric processing.
- Deletion within 30 days of all existing biometric collections.
- Cessation of effect of this Addendum.

Article 14 — Articulation with the Main DPA

This Addendum is annexed to the main DPA concluded between the Parties and forms an integral part of it. The provisions of the main DPA apply to all processing not specifically governed by this Addendum.

In case of contradiction between the main DPA and this Addendum, the provisions of this Addendum prevail with regard to biometric processing.

Attimo — Frédéric Gras Photographe — SIRET 453 606 253 00020
38 avenue de Tournaisis, 78990 Élancourt, France
info@attimo-gallery.com — attimo-gallery.com