Data Processing Agreement (DPA Art. 28 GDPR)

Version v3.2

En vigueur depuis le 03 novembre 2026

Publié le 03 novembre 2026

Langue : EN

Data Processing Agreement (DPA)

Attimo Platform — attimo-gallery.com
Version 3.2 — November 2026
Article 28 of Regulation (EU) 2016/679 (GDPR)

Between the undersigned

The Controller (“the Client”)

The professional photographer (natural or legal person) who has subscribed to the Attimo Platform, whose details are recorded in their personal account on the Platform.

Hereinafter referred to as “the Controller” or “the Client”.

The Processor

- **Name:** Frédéric Gras Photographe — trading name: Attimo
- **Legal status:** Sole trader (Entrepreneur individuel — EI)
- **Address:** 38 avenue de Tournaisis, 78990 Élancourt, France
- **SIRET:** 453 606 253 00020
- **General / GDPR email:** info@attimo-gallery.com
- **Technical support email:** support@attimo-gallery.com

Hereinafter referred to as “the Processor” or “Attimo”.

The Controller and the Processor are hereinafter collectively referred to as “the Parties” and individually as “a Party”.

Preamble

The Parties have entered into a main agreement governing the use of the Attimo Platform (hereinafter “the Main Agreement”), embodied in Attimo's Terms of Use and Sale.

In performing this Main Agreement, the Processor processes personal data on behalf of the Controller.

In accordance with Article 28 of Regulation (EU) 2016/679 of 27 April 2016 (GDPR), the Parties wish to govern the conditions of such processing through this Data Processing Agreement (hereinafter “the DPA”).

This DPA is appended to Attimo's Terms of Use and Sale and forms an integral part thereof. It is deemed accepted by the Client upon registration on the Platform.

i Changes introduced in version 3.2. This version adds LiveKit to the list of sub-processors, for the video calls of Attimo Studio connected sessions, and specifies the related transfers outside the European Union.

i Changes introduced in version 3.1. This version specifies the retention periods of the facial templates of the Sport module for sports clubs (players' identity photos, match photos in the batch to be sorted retained for a maximum of thirty days), detailed in the Biometric Addendum.

i Changes introduced in version 3.0. This version incorporates the Attimo Studio and Vintage Photo Restoration modules, updates the list of sub-processors, specifies the retention periods applicable to each category of data, and documents the transit of payment events associated with Stripe Connect.

Article 1 — Purpose

The purpose of this DPA is to define the conditions under which Attimo, acting as processor, processes on behalf of the Client, acting as controller, the personal data required to deliver the services of the Attimo Platform.

It sets out in particular:

- The nature and purpose of the processing operations.
- The categories of data and of data subjects.
- The retention periods applied.
- The obligations and responsibilities of each Party.
- The security measures implemented.
- The use of sub-processors.

- The arrangements for exercising data subject rights.

Article 2 — Definitions

Terms used in this DPA have the meaning given to them by the GDPR. In particular:

- "**Personal data**": any information relating to an identified or identifiable natural person.
- "**Processing**": any operation performed on personal data (collection, recording, storage, alteration, disclosure, erasure, etc.).
- "**Controller**": the person who determines the purposes and means of the processing.
- "**Processor**": the person who processes personal data on behalf of the controller.
- "**Personal data breach**": any breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data.
- "**Data subjects**": the natural persons whose data is processed (end clients of the galleries, visitors, buyers, session participants, persons appearing in the photographs).
- "**Anonymisation**": the irreversible erasure of the elements enabling identification of a person, such that the residual data no longer constitutes personal data within the meaning of the GDPR.

Article 3 — Description of the processing

3.1 Nature and purpose of the processing

Attimo processes the personal data supplied by the Client or collected through the Platform for the following purposes:

- Hosting and delivery of online photographic galleries.
- Management of end client access to galleries (access codes, favourites, selections).
- Management of orders, baskets and payments.
- Sending of transactional communications (emails, SMS).
- Preparation of production files and shipment of physical orders.
- Delivery of the features specific to the modules activated by the Client, in particular:
  - **Sport**: identification of participants by bib number reading and, where applicable, facial recognition; for a sports club, recognition of the authorised players in match photos based on their identity photo (see Biometric Addendum).
  - **School and Nursery**: management of individual galleries and parental authorisations (see Minors Data Addendum).
  - **Studio**: organisation of in-person or remote reveal sessions, artwork composition, collection of the electronic signature on the order form, video calls during connected

sessions (voice and image transmitted live, without recording; Attimo keeps the display name, times and length of presence).
    - **Vintage Photo Restoration**: automated repair processing of images entrusted by the Client, under the Client's control and subject to the Client's validation of each result.
    - **Video, File Transfer, Art Gallery, Photo Book, Gift Cards**: hosting, delivery and sale of the corresponding content.
- Handling of requests submitted to Attimo's technical support.
- Backup and retention of data for the periods set out in Article 3.4.

3.2 Categories of data subjects

The processing carried out under this DPA concerns the following categories of persons:

- The end clients of the Client's photographic galleries (buyers, guests).
- The subjects of the photographs, under the Client's responsibility.
- Participants in Studio reveal sessions, whether in person or remote.
- Persons appearing in the vintage photographs entrusted to the Restoration module, including deceased persons or unidentifiable third parties.
- Persons submitting a request to Attimo's technical support.
- Any partners or suppliers of the Client whose contact details are recorded on the Platform.

3.3 Categories of data processed

Category of data	Detail	Sensitive
Identification data	Surname, first name, email, telephone, address	No
Order data	Items, amounts, history	No
Payment data	Payment method, transaction status, last four digits of the card. Full banking details never pass through the Platform and are handled by the payment providers.	No
Browsing data	IP address, user agent, timestamp, pages viewed, usage statistics	No
Photographs	Content of galleries and sessions (visible persons)	Depending on content
Vintage photographs (Restoration module)	Images entrusted by the Client for automated repair, which may depict identifiable persons, including deceased persons	Depending on content

Category of data	Detail	Sensitive
Electronic signature (Studio module)	Handwritten mark of the end client affixed to the order form, timestamp, IP address	No — evidential data
Connected session data (Studio module)	Participant name, association with a buyer, individually attributed favourites	No
Support correspondence	Content of inbound emails sent to support, attachments, sender address	Depending on content
Biometric data (Sport module)	Facial templates via AWS Rekognition	Yes — Art. 9 GDPR
Data relating to minors (School / Nursery modules)	Children's identity (first name, class), parents' contact details for sending access codes and digital parental authorisations (Nursery module only)	Protected — Art. 8 GDPR

i In the School module, the collection of parental authorisations is handled directly by the school (primary controller). Attimo processes parents' contact details solely to send access codes to pupils' individual galleries.

In the Nursery module, the Client may use the digital parental authorisation system built into the Platform. In that case, Attimo processes parents' email addresses in order to obtain their prior consent on behalf of the Client. Where the Client collects authorisations by other means, Attimo does not process consent data.

⚠ **The processing of biometric data and of data relating to minors is governed by specific Addenda to this DPA**, accepted by the Parties upon activation of the modules concerned.

3.4 Retention periods

Processing is carried out for the entire duration of the Main Agreement. Each category of data is retained for the period indicated below, after which it is deleted or anonymised by automated procedures.

Category of data	Retention period	Basis
Gallery photograph files	Gallery lifespan set by the Client, plus a one-month grace period, then deletion within 30 days	Product design and data minimisation (Art. 5.1 GDPR)
Studio session files	6 months after the session (period configurable by the Client)	Data minimisation
Restoration module working files	30 days after validation by the Client	Data minimisation

Category of data	Retention period	Basis
Transfer files	Expiry period set by the Client, automatic deletion upon expiry	Data minimisation
Order data and accounting records	10 years	French Commercial Code, Art. L. 123-22
Electronic signature on the order form	10 years, attached to the order for which it serves as evidence	Evidential value
Gallery access logs	Identifying elements (IP address, user agent, email) anonymised at 6 months; residual record deleted at 24 months	CNIL recommendation and retention of aggregated statistics
Technical logs (login, download, two-factor authentication, carrier interface calls, Support module)	6 months	CNIL recommendation
Notification delivery logs (emails, SMS)	6 months	CNIL recommendation
Cookie consents	13 months	CNIL Decision No. 2020-091
Evidence of acceptance of legal documents	5 years after the end of the Main Agreement	French Commercial Code, Art. L. 110-4
Facial templates (Sport module, events)	Deleted when the event or gallery is closed; automatic daily purge	Art. 9 GDPR — see Biometric Addendum
Facial template of a club player's identity photo (Sport module)	As long as the player is part of the team; deleted when the authorisation is refused, when the photo is changed or removed, or when the player or the team is removed	Art. 9 GDPR — see Biometric Addendum
Facial templates and jersey numbers read in a club's match photos (Sport module)	A maximum of 30 days after the first analysis of the batch to be sorted; deleted immediately when the batch is emptied; automatic daily purge	Art. 9 GDPR — see Biometric Addendum
Evidence of consent to biometric processing	5 years (adults) — 20 years (minors)	See Biometric Addendum
Digital parental authorisations (Nursery module)	5 years	French Civil Code, Art. 2224 — see Minors Addendum
Client account (settings, configurations)	30 days after the effective date of termination	See Article 11

i Gallery access logs are anonymised rather than deleted at six months. This anonymisation

is irreversible: the IP address, the user agent and any associated email address are permanently overwritten. All that remains is a view counter stripped of any identifying element, which preserves the statistical history made available to the Client.

Article 4 — Obligations of the Processor

Attimo undertakes to:

1. Process personal data solely for the purposes described in Article 3 and on documented instructions from the Client.
2. Inform the Client immediately if, in Attimo's view, an instruction received infringes the GDPR or any other data protection provision.
3. Ensure the confidentiality of the personal data processed and ensure that persons authorised to process the data are bound by a duty of confidentiality.
4. Implement the appropriate technical and organisational measures set out in Article 6 to ensure a level of security appropriate to the risk.
5. Assist the Client in meeting its GDPR obligations, in particular in responding to requests from data subjects exercising their rights.
6. Notify the Client of any personal data breach within 48 hours of becoming aware of it.
7. Refrain from exploiting for its own purposes the photographs, files and end client data hosted on behalf of the Client, in particular for communication, commercial demonstration or algorithmic model training, save with the written, separate and revocable authorisation of the Client.
8. Not engage sub-processors without complying with the conditions set out in Article 7.
9. Make available to the Client all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR.
10. Allow for and contribute to audits, including inspections, conducted by the Client or an auditor mandated by the Client, under the conditions set out in Article 8.

Article 5 — Obligations of the Controller

The Client undertakes to:

1. Provide Attimo with the information required to carry out the processing and ensure the accuracy, adequacy and relevance of the data transmitted.
2. Ensure that the processing carried out complies with the principles set out in the GDPR (lawfulness, fairness, transparency, minimisation, accuracy, storage limitation, integrity and confidentiality).
3. Inform the data subjects of the processing carried out, in accordance with Articles 13 and

14 of the GDPR, in its own terms and policies. This information covers in particular gallery audience measurement, the use of an automated image processing provider where the Restoration module is used, and the collection of the electronic signature where the Studio module is used.

4. Obtain the necessary consents where the legal basis for processing is the data subject's consent, in particular for biometric processing (Art. 9 GDPR) and processing relating to minors (Art. 8 GDPR).
5. Warrant that it holds the necessary rights and authorisations over all content it uploads, including photographs entrusted to the Restoration module, music played during sessions and imported graphic elements.
6. Control the distribution of the session and gallery links it circulates, such links granting access to the corresponding content.
7. Document in writing the instructions given to Attimo and keep evidence available at the request of the supervisory authorities.
8. Verify, before and throughout the processing, the Processor's compliance with GDPR obligations.
9. Supervise the processing through audits and inspections of the Processor.
10. Assume full responsibility for the processing carried out, in particular by responding to requests from data subjects and supervisory authorities.

Article 6 — Security measures

In accordance with Article 32 of the GDPR, Attimo implements the following technical and organisational measures to ensure a level of security appropriate to the risk:

6.1 Technical measures

- Password hashing using the bcrypt algorithm (cost factor 14 — high security).
- Secure HTTPS/TLS connections with Let's Encrypt certificates across the entire Platform.
- Strict data isolation between Clients through a multi-tenant architecture: systematic filtering by Client identifier on every query, every model and every storage path.
- Access to media files through temporary, cryptographically signed URLs (HMAC) with short expiry. Direct storage addresses are never exposed, the storage container not being public.
- Two-tier token system for connected sessions: a shared viewing token and a personal token required to place an order.
- Encryption in the database of the credentials for third-party services configured by the Client.

- Regular automated backups of databases and application files, distributed across several separate infrastructures.
- Regular updating of software components (Laravel, PHP, dependencies) and of the operating system.
- Protection against common attacks: anti-CSRF tokens on all forms, protection against script injection, prepared statements against SQL injection, sanitisation of vector content served.
- Limitation of login attempts and rate limiting on sensitive routes (authentication, signature, payment).
- Two-factor authentication available for Client accounts.
- Deterrent measures against unauthorised downloading of photographs (right-click and drag-and-drop blocking) and application of a watermark to public galleries where the Client has enabled that option.
- Logging of access and sensitive actions, with automatic purging or anonymisation at the intervals set out in Article 3.4.
- Pre-production environment strictly separated from the production environment.
- Continuous application monitoring and alerting in the event of operational anomalies.

⚠ **Scope of the watermark.** The watermark is a commercial deterrent, not a security measure within the meaning of Article 32 of the GDPR. It is not applied to images displayed during Studio reveal sessions, whether in person or remote, as those images are intended to be presented by the Client to its own clients in a setting the Client controls. The Client is informed of this so as to take it into account when circulating session links.

6.2 Organisational measures

- Access to data strictly limited to persons authorised in the course of their duties.
- Confidentiality undertaking from persons accessing the data, including the managed hosting provider.
- Documented procedure for notifying data breaches.
- Data retention policy consistent with the periods set out in Article 3.4, enforced by automated daily tasks.
- Isolation of Support module logs in a dedicated channel, so as to circumscribe the processing of inbound correspondence.
- Record of processing activities kept up to date in accordance with Article 30 of the GDPR.

6.3 Data location

Personal data is hosted and processed exclusively within the European Union:

- Application databases and media files: OVH SAS, Gravelines, France.
- Facial recognition processing, Sport module only: Amazon Web Services, Europe region — Ireland (eu-west-1).
- Automated image restoration processing, Restoration module only: Nero AG, own data centre located in Germany.

No transfer of personal data outside the European Union is carried out by Attimo in connection with the hosting and processing of data. Payment providers engaged at the Client's initiative may, for their part, carry out transfers governed by appropriate safeguards such as standard contractual clauses or the Data Privacy Framework. The Attimo Studio video call, when used by the Client, relies on LiveKit Incorporated (United States): voice and image may transit through servers located outside the European Union, without being stored there. This transfer is governed by LiveKit's data processing addendum (Data Privacy Framework and, failing that, the European Union standard contractual clauses).

Article 7 — Use of sub-processors

7.1 General authorisation

The Client authorises Attimo to engage the following sub-processors for the performance of the processing:

Sub-processor	Service	Location
OVH SAS	Hosting of the website and application, media file storage, backups	France (Gravelines, Roubaix)
Cognix Systems	Managed server hosting: system administration, monitoring, maintenance, backups. Holds administrator access to the production infrastructure.	France
Amazon Web Services EMEA SARL	Facial recognition (Sport module only)	Ireland (eu-west-1)
Nero AG	Automated image restoration and upscaling processing (Restoration module only)	Germany (Karlsruhe)
Stripe Payments Europe	Card payments and collection on behalf of third parties (Stripe Connect)	Ireland
SystemPay (Lyra Network)	Card payments	France
PayPal Europe	PayPal payments	Luxembourg
Mollie B.V.	Payments	Netherlands

Sub-processor	Service	Location
Attimo mail server	Sending of transactional emails from Attimo's server	France (Gravelines)
LiveKit Incorporated (if the Client uses the Attimo Studio video call)	Video calls during connected sessions, without recording	United States; session data in the European Union (Frankfurt), voice and image may transit outside the EU without being stored there
Brevo — Sendinblue SAS (if enabled by the Client)	Large-scale email delivery	France / EU
SMS Envoi	Sending of transactional SMS messages	France
Mondial Relay	Order shipping and delivery tracking (if enabled by the Client)	France
Koy Lab (if enabled by the Client)	Professional printing of albums and photographic prints	Portugal

i The sub-processors listed above represent all providers that may be engaged by Attimo. Some are active by default; others are engaged only where the Client activates a specific feature (Amazon Web Services for the Sport module, Nero AG for the Restoration module, Brevo for large-scale email delivery, Mondial Relay for shipping, Koy Lab for printing).

In addition, Clients may configure their own mail server for the communications sent from their workspace. In that case, the provider chosen by the Client becomes a sub-processor under the Client's own responsibility.

7.2 Addition or replacement

Attimo shall inform the Client by any appropriate means (email, notification on the Platform, update of this list) of any intended addition or replacement of a sub-processor, within a reasonable period before implementation.

The Client has 15 days in which to raise reasoned objections. In the absence of an objection within that period, the addition or replacement is deemed accepted.

In the event of a reasoned objection, the Parties shall confer to find a solution. Failing agreement, the Client may terminate the Main Agreement under the conditions provided for.

7.3 Attimo's obligations towards its own sub-processors

Attimo ensures that each sub-processor it engages provides sufficient guarantees as to the implementation of appropriate technical and organisational measures. Attimo enters into written contracts with each of these sub-processors imposing obligations equivalent to those

in this DPA.

Attimo remains fully liable to the Client for the performance by its sub-processors of their obligations.

7.4 Automated image processing in the Restoration module

Where the Client uses the Restoration module, the images uploaded are transmitted to Nero AG solely for the purpose of automated processing. The Parties agree as follows:

1. Transmission takes place only at the Client's initiative, image by image, upon each processing request.
2. Processing is carried out exclusively on Nero AG's own infrastructure located in Germany, without recourse to any third-party cloud provider.
3. Images transmitted are deleted by Nero AG within eight hours of processing.
4. Images transmitted are not used for algorithmic model training.
5. The result is retrieved onto Attimo's infrastructure as soon as it is produced, then submitted to the Client for validation. No result is delivered without the Client's prior review.

⚠ **Nature of the processing.** Restoration relies on generative processing: in an area where the information has physically disappeared, the tool produces a plausible reconstruction rather than a faithful reproduction of the original. The result may therefore not be presented as an identical restoration. That is why every result is submitted to the Client for validation before delivery, such validation being a matter for the Client's professional judgement alone.

7.5 Transit of payment events collected on behalf of third parties

Where the Client connects its Stripe account to the Platform in order to collect its own sales directly, the Platform receives from Stripe the notifications of events occurring on that account. The Parties agree as follows:

1. This connection is technically necessary: as payments are collected directly into the Client's account, the corresponding notifications originate on that account and not on Attimo's. Without them, no order could be confirmed.
2. Stripe does not allow these notifications to be filtered by origin. Attimo therefore receives, in transit, all payment and refund notifications occurring on the Client's account, including those arising from the Client's own professional activity and unrelated to the Platform.
3. The data thus received is limited to the amount, the currency, the transaction status and, where applicable, the end client's email address and the last four digits of the card. No full card number is transmitted.

4. Any notification lacking the Platform's own origin marker is rejected without any write to the database. All that remains is a technical log entry, subject to the six-month purge provided for in Article 3.4.
5. A Client seeking complete separation of its activities may dedicate a separate Stripe account to its use of the Platform. This is a recommendation, not an obligation.

7.6 Specific case of sub-processors under the Client's own account

Certain sub-processors are engaged only at the Client's own initiative, the Client then contracting directly with them to obtain their services. This applies in particular to payment providers, to the Brevo service where the Client selects that transport for sending its emails, to the carrier Mondial Relay, and to the accounting synchronisation tools to which the Client exports its data.

In that specific case, the Parties expressly agree as follows:

1. The account with the sub-processor under the Client's own account is opened, held and paid for directly by the Client.
2. The main contract between the Client and that sub-processor (terms of use, privacy policy, the sub-processor's own data processing agreement) is the Client's sole responsibility. The Client acknowledges having read and accepted those documents when opening the account.
3. Attimo's role is limited to that of a technical gateway transmitting the credentials entered voluntarily by the Client. Those credentials are stored encrypted in the database, in accordance with the technical measures described in Article 6.
4. The Client may discontinue use of that sub-processor at any time by changing the corresponding configuration in its settings. Doing so immediately suspends any transmission of data to the sub-processor concerned.
5. Data exports triggered by the Client towards a third-party tool are carried out at the Client's sole initiative and under the Client's sole responsibility. Attimo has no control over the downstream processing performed by the recipient.
6. Attimo shall not be held liable for the processing of data carried out directly by that sub-processor in performance of the contract concluded between it and the Client, nor for any failure by that sub-processor to meet its own GDPR obligations.

Article 8 — Audits and inspections

The Client may carry out, or have carried out, audits of Attimo's compliance with the obligations under this DPA, subject to the following conditions:

1. The audit is announced in writing at least 30 days before it takes place.

2. The audit is conducted during business hours and must not disrupt the normal operation of the Platform.
3. Audit costs are borne by the Client, unless the audit reveals a significant failure on Attimo's part.
4. The auditor is bound by a confidentiality obligation equivalent to that of the Parties.
5. Attimo may object to the appointment of a competing auditor.

In lieu of an on-site audit, Attimo may make available to the Client certifications, audit reports or documents attesting to its compliance.

Article 9 — Personal data breaches

9.1 Notification

In the event of a personal data breach (unauthorised access, data loss, leak, etc.), Attimo shall notify the Client within a maximum of 48 hours of becoming aware of it. That notification shall contain at least:

- A description of the nature of the breach (categories and approximate volume of data and data subjects concerned).
- The likely consequences of the breach.
- The measures taken or proposed to address the breach and mitigate its effects.
- The contact point for obtaining further information.

9.2 Cooperation with the supervisory authority

Attimo shall cooperate fully with the Client to enable it, where applicable:

- To notify the breach to the supervisory authority within 72 hours (Article 33 GDPR).
- To inform the data subjects where the breach is likely to result in a high risk to their rights and freedoms (Article 34 GDPR).

9.3 Documentation of incidents

Attimo maintains an internal register documenting any personal data breach in accordance with Article 33.5 of the GDPR. That register records the description of the facts, the effects observed and the corrective measures taken.

The register is made available to the supervisory authority in the event of an inspection.

Article 10 — Data subject rights

Attimo makes available to the Client the technical tools required to enable data subjects to exercise their rights (access, rectification, erasure, restriction, portability, objection).

If a data subject addresses a request to Attimo directly, Attimo shall forward it to the Client within 5 working days, unless the request relates exclusively to processing carried out by Attimo as a separate controller (see Privacy Policy).

The Client remains solely responsible for responding to data subject requests relating to its own processing, within the statutory time limits.

Article 11 — Fate of the data at the end of the contract

In accordance with Attimo's Terms of Use and Sale, upon the end of the Main Agreement, for whatever reason, Attimo shall proceed as follows:

1. Access to the Platform is immediately and permanently cut off.
2. All of the Client's data hosted on the Platform is permanently deleted from Attimo's systems, including from backups, within a maximum of 30 days from the effective date of termination.
3. Attimo may provide the Client, upon express written request, with a certificate of effective data deletion.

By way of exception, certain data may be retained beyond that period where such retention is required by a legal obligation, in particular accounting data relating to subscription invoicing, retained for 10 years, and evidence of acceptance of the legal documents, retained for 5 years.

i As the Client keeps its source photographic files on its own equipment (hard drives, editing software), no file export procedure is required before termination of the Main Agreement. The Client is, however, invited to export its business data (orders, statistics) using the tools made available, under the conditions set out in the Terms of Use and Sale.

Article 12 — Digital sobriety commitment

The permanent deletion of personal data at the end of the contractual relationship, provided for in Article 11 of this DPA, serves two complementary requirements.

First, the storage limitation principle laid down in Article 5.1 of the GDPR, which requires personal data to be kept only for as long as is strictly necessary to fulfil the purposes for which it is processed.

Second, a voluntary commitment by Attimo to digital sobriety. The prolonged retention of personal data, photographic files and backups entails a continuous consumption of energy and material resources. Attimo considers that the effective deletion of data once its legitimate usefulness has ended is sound environmental practice, complementary to regulatory obligations.

To that end, Attimo has chosen an infrastructure hosted in France (OVH Gravelines) that prioritises energy efficiency, and implements automated deletion procedures that effectively release storage resources upon expiry of the retention periods.

This approach is aligned with the spirit of the general reference framework for the eco-design of digital services (RGESN) published by Arcep and the French interministerial digital directorate (DINUM).

Article 13 — Liability

Each Party is liable for damage resulting from the breach of its own obligations under the GDPR and this DPA.

In the event of joint liability towards a data subject or a supervisory authority, the Party that has borne the compensation may seek recourse against the other Party in proportion to its share of liability.

Attimo's liability under this DPA is capped under the conditions set out in the Terms of Use and Sale, except in cases of wilful misconduct or gross negligence.

i Attimo shall not be held liable for the Client's failure to meet its own obligations (obtaining consent, informing data subjects, respecting image rights, holding the rights to uploaded content, etc.). The Client shall indemnify Attimo against any third-party claim arising from such a failure.

Article 14 — Term and amendments

This DPA takes effect on the date of acceptance by the Client (upon registration on the Platform or upon acceptance of a new version) and remains in force for the entire duration of the Main Agreement.

Attimo may amend this DPA in order to comply with legislative, regulatory or case-law developments in the field of data protection, as well as to reflect changes in the Platform's features. Any substantial amendment is notified to the Client with a minimum of 30 days' notice before it takes effect.

Should the Client refuse the amendments, it may terminate the Main Agreement without penalty before the amendments take effect.

Article 15 — Governing law and jurisdiction

This DPA is governed by French law and by Regulation (EU) 2016/679 (GDPR).

Any dispute relating to the interpretation or performance of this DPA shall be submitted to the competent courts under the conditions set out in Attimo's Terms of Use and Sale.

Article 16 — Acceptance

This DPA is accepted by the Client upon registration on the Attimo Platform by means of a checkbox separate from the acceptance of the Terms of Use and Sale.

Electronic acceptance constitutes signature of this DPA and fully binds the Parties.

ℹ Attimo retains evidence of the Client's acceptance of the DPA (date, time, IP address, version accepted) in its database. This evidence may be provided at the request of the Client or of the supervisory authorities.

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