Data Processing Agreement (DPA)

Last updated: 27 May 2026

> ***Translation notice:*** *this English version of the Data Processing Agreement is a translation provided for information purposes only. Only the original French version is legally binding. In the event of any discrepancy between this translation and the French version, the French version shall prevail.*

Preamble

This Data Processing Agreement (the "**Agreement**" or "**DPA**") forms an integral part of the General Terms of Sale and Use (the "**Terms**") and applies between:

- eCapitalio, a French simplified joint-stock company (société par actions simplifiée) with a share capital of €44,286.88, registered with the Nanterre Trade and Companies Register under number 827 483 462, whose registered office is located at 18 rue de la ferme, 92200 Neuilly-sur-Seine, France (hereinafter "We"); and
- the Client who has subscribed to the Contract (hereinafter "You").

We and You are hereinafter jointly referred to as the "Parties".

Compliance commitments

The Parties undertake to comply with the applicable regulations on the protection of personal data and, in particular, the French **Data Protection Act (loi Informatique et Libertés)** as amended on 20 June 2018 and **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 (the "**GDPR**").

We apply a personal data protection policy whose characteristics are set out in the document entitled **"Privacy Policy"**, which You are expressly invited to read.

Roles of the Parties and Purpose

It is agreed that **You will act as data controller** and that **We will act as data processor** in the context of the provision of the Services. This Agreement reflects the Parties' commitments regarding the processing of your Personal Data by Us as Processor.

The provisions applicable between a Controller and a Processor apply only to the extent that We process your Personal Data in connection with the Subscription Contract.

Order of precedence and Updates

In the event of any conflict or inconsistency with the provisions of the Terms, this Agreement shall prevail over the Terms solely with respect to the matters concerned.

This Agreement is updated regularly. If You have an active subscription, We will inform You of such updates by email. Archived versions of this Data Processing Agreement can be found in the website archives, available on the dedicated page of the website.

The term of this Data Processing Agreement shall be the same as that of the Terms. Terms not otherwise defined in this section are defined in the Terms.

Article 1 - Definitions

- **Administrator**: an officer or employee of your company, or a third party expressly authorised by You, to access the Data and to modify/delete it via a specific Account called the "Administrator Account" which is personal to them and who, by virtue of their position, may manage the shareholding of your company.
- **Application**: the electronic means We provide to You in order to access the Services, i.e. access to the website available at https://www.equify.eu which We operate (and/or any other website of which You may subsequently be informed), or any application that may be operated on a mobile device and that We may make available to You.
- **Account**: secure space containing all of your Data and accessible via the Application.
- **Contract**: these general terms and conditions of sale and use, the Subscription Contract, and the subscription prices applicable on the date of subscription and appended to your Subscription Contract.
- **Subscription Contract**: document setting out the specific contractual terms of the Services to which You have subscribed.
- **Data**: all content (including personal data), information, text, images, photographs, audio content, video content and any other content, document and component, in whatever format, provided by You or any of your Users in connection with the configuration of the Account and/or the use of the Services.
- **Services**: all the services We provide to You within the scope of the Services set out in the Subscription Contract, including access to and use of the Application.
- **Holder**: any natural or legal person duly identified as a "Holder" on the Application by an Administrator of the Account by reason of the current, future or past ownership of financial securities of your company.
- **Users**: any person logging in with their personal credentials to the Application and who has been granted access to the Account.

Article 2 - Your Responsibility

2.1. Compliance with the law. In your capacity as data controller, You warrant to Us that You have fulfilled all the obligations incumbent upon You and that You have informed the data subjects of the use made of such personal data.

Likewise, as data controller, You are responsible for the accuracy, quality and lawfulness of the personal data You transfer to Us, as well as for the means by which You obtained such personal data.

Accordingly, You shall indemnify Us against any action, complaint or claim from any natural person whose personal data is reproduced and hosted via the Application.

2.2 Instructions. You are responsible for ensuring that the instructions You give Us regarding the processing of your Personal Data comply with applicable laws, including Data Protection Laws. The Parties agree that the Terms (including this Agreement), together with your use of the Subscription Service in accordance with the Terms, constitute your complete Instructions to Us regarding the processing of your Personal Data by Us, insofar as You may give, during the subscription term, additional instructions consistent with the Terms and with the nature and lawful use of the Subscription Service.

2.3 Security. You must independently determine whether the data security measures provided as part of the Subscription Service adequately meet your obligations under Data Protection Laws. You are also responsible for your secure use of the Subscription Service, including protecting the security of Personal Data in transit to and from the Subscription Service (including by securely backing up or encrypting such Data).

Article 3 - Our Obligations as Processor

3.1 Compliance with Instructions. We undertake to process Your Personal Data only for the purposes described in this Data Processing Agreement or as agreed under your lawful Instructions, unless otherwise required by law.

If We consider that an instruction infringes the GDPR or any other provision of Union or Member State law relating to data protection, We will inform You immediately.

3.2 Security. We implement and maintain appropriate technical and organisational measures to protect your Personal Data against any breach, as described in our "Internal Security Policy" ("Security Measures"). Notwithstanding anything to the contrary, We may modify or update the Security Measures at our sole discretion, provided that such modification or update does not result in a material degradation of the protection afforded by the Security Measures.

3.3 Confidentiality. We undertake to ensure that all personnel whom We authorise to process your Personal Data on your behalf are subject to appropriate confidentiality obligations (whether contractual or statutory) with respect to such Data and receive the necessary training in personal data protection (see "Employee Privacy Policy").

Subject to the provisions of Article 6 "Liability" of the Terms, We undertake to preserve the integrity and confidentiality of the Data contained in the Application. We will implement technical and organisational measures designed to prevent any fraudulent access to or use of the Data and to prevent any loss, alteration or destruction of the Data. These measures are detailed in ***"Appendix 3: Quality Charter"***.

3.4 Personal Data Breaches

We will notify You of any personal data breach within a maximum of forty-eight (48) hours after becoming aware of it, by email to the email address You have provided for this purpose. This notification will be accompanied by any relevant documentation to enable You, where necessary, to notify the breach to the competent supervisory authority and, where applicable, to the data subjects affected by the personal data breach.

As data controller, where necessary, carrying out data protection impact assessments and prior consultation of the supervisory authority, as provided for by the GDPR for your processing operations, is your responsibility. Nevertheless, We will assist You, where necessary in light of the requirements of the supervisory authorities, in particular the French Data Protection Authority (Commission Nationale Informatique et Libertés, CNIL), in fulfilling these obligations by providing You with all necessary information, as described in our "Personal Data Breach Management Policy".

3.5 Deletion or return of Personal Data. At the end of the Subscription Contract, We undertake, at your choice, to destroy or return to You all personal data processed on your behalf for the purpose of performing the Services.

If this option is chosen, the return must be accompanied by the destruction of all existing copies in our information systems.

3.6. Data Protection Officer. For any request relating to the processing of personal data, You may contact our Data Protection Officer by email at **dpo@equify.eu**.

3.7 Record of categories of processing activities. We declare that We keep a written record of all categories of processing activities carried out on your behalf.

Upon your express request, and subject to the confidentiality obligations set out in the Contract, We undertake to make available to You the information necessary to demonstrate compliance with the obligations set out in this article and arising directly from the GDPR. In addition, upon request, We will also allow You, at your own expense, to carry out audits of the processing activities covered by the Contract.

Article 4 - Data subject requests

To the extent possible, We must assist You in fulfilling your obligation to respond to requests from data subjects exercising their rights:

- right of access
- right to rectification
- right to erasure
- right to object
- right to restriction of processing
- right to data portability
- right not to be subject to automated individual decision-making (including profiling)

Where data subjects submit requests to Us to exercise their rights, We must forward such requests to You upon receipt, by email to the email address You have provided for this purpose, as soon as possible, as described in our "Data Subject Access Rights Policy".

Article 5 - Sub-processors

You authorise Us to engage sub-processors to carry out specific processing activities, the list of which is set out in our **Privacy Policy**.

We may engage other Sub-processors to carry out specific processing activities. In such a case, We will inform You in advance and in writing of any intended change concerning the addition or replacement of the Sub-processors listed in our **Privacy Policy**.

In any event, You have a minimum period of 30 days from the notification to raise your objections.

Such sub-processing may only take place if the controller has not raised any objection within the agreed period.

It is our responsibility to ensure that the Sub-processor provides the same sufficient guarantees as to the implementation of appropriate technical and organisational measures so that the processing meets the requirements of the GDPR.

If the Sub-processor fails to fulfil its data protection obligations, We remain fully liable to You for the performance of the other processor's obligations.

Article 6 - Data transfers

Data is mainly processed within the European Union. If a transfer to a third country is necessary, We ensure that the transfer complies with Data Protection Laws, in particular through the use of Standard Contractual Clauses.

If We are required to transfer data to a third country or an international organisation under Union or Member State law to which We are subject, We will inform You of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

Article 7 - Proof of compliance

We will make available to You all information reasonably necessary to demonstrate our compliance with this Agreement, and We will allow for and contribute to audits, including inspections by You or your auditor, in order to assess compliance with this Agreement where required by applicable law.

You acknowledge and agree that You shall exercise your audit rights under this Agreement by instructing Us to comply with the measures described in this "Proof of compliance" section.

You acknowledge that the Subscription Service is hosted by our Sub-processors, which maintain independently validated security programmes (including SOC 2 and ISO 27001).

In addition, upon your written request, We will provide written responses (on a confidential basis) to all reasonable requests for information necessary to confirm our compliance with this Agreement, provided that You do not exercise this right more than once per calendar year, unless You have reasonable grounds to believe that We are not complying with this Agreement.

Article 8 - General provisions

8.1 Order of precedence. In the event of any conflict or inconsistency between the provisions of this Agreement and the Terms, this Agreement shall prevail solely with respect to the Processing of Personal Data.

8.2 Amendments. We reserve the right to update this Agreement (for example, to adapt to legislative changes). We will inform You by notification in the Application or by email. If You continue to use the Services after such notification, You shall be deemed to have accepted the amendments.

8.3 Limitation of liability. Each party's (Ours and Yours) aggregate liability arising out of this Agreement is subject to the limitations and exclusions of liability set out in the Terms. In no event shall this clause limit the rights of individuals (data subjects) under the GDPR.

8.4 Severability. If any provision of this Agreement is held invalid or unenforceable by a court, the remainder of the Agreement shall remain in full force and effect.

8.5 Governing law. This Agreement is governed by French law. Any dispute relating to its interpretation or performance shall fall within the jurisdiction of the courts of the place of our registered office, unless otherwise mandatorily provided by Data Protection Laws.

Article 9 - Parties to this Data Processing Agreement

9.1 Authorised Affiliates. By accepting the Terms, You enter into this Agreement on your own behalf and also in the name and on behalf of your Authorised Affiliates (any entity related to You and authorised to use the Services). For the purposes of this Agreement, the term "You" refers collectively to the signatory entity and its Authorised Affiliates.

9.2 Authority. You represent and warrant that You are duly authorised to enter into this Agreement on your own behalf and on behalf of your Authorised Affiliates.

9.3 Management of claims and communications. The Parties agree that:

- (i) Only the signatory entity may exercise rights of recourse or audit on behalf of its Authorised Affiliates.
- (ii) You are responsible for coordinating all instructions and communications with Us. We shall be discharged from our obligations by communicating directly with You on behalf of the group.

Appendix 1: Information about the processing - We act as processor

1. List of parties

Data exporter:

Name: You, as defined in the Terms (on its own behalf and on behalf of its Authorised Affiliates)

Address: your address, as indicated on the quote

Contact person's name, role and contact details: your contact details, as indicated on the quote and/or in your Account.

Activities relevant to the data transferred under these Clauses: processing of your Personal Data in connection with your use of the Subscription Services, in accordance with the Terms.

Role (controller/processor): Controller (either as controller, or acting as controller or as processor on behalf of another controller).

Data importer:

Name: eCapitalio SAS (trading as Equify)

Address: 18, rue de la ferme, 92200 NEUILLY-SUR-SEINE, France

Contact person's contact details: **dpo@equify.eu**

Activities relevant to the data transferred under these Clauses: processing of your Personal Data in connection with your use of our Subscription Services, in accordance with the Terms.

Role (controller/processor): Processor

2. Description of the transfer

You may submit Personal Data to the Subscription Services, the extent of which is determined and controlled by You in your sole discretion, and which may include, without limitation, Personal Data relating to the following categories of data subjects:

- Your shareholders, partners and securities holders (natural persons);
- Your employees and staff (beneficiaries of employee share plans such as BSPCE, free shares (AGA) and stock options);
- Your corporate officers, directors and members of management bodies;
- Your authorised advisers and third-party service providers (lawyers, chartered accountants);
- Any end user authorised by You to use the Subscription Service.

Categories of Personal Data transferred

You may submit Personal Data to the Subscription Services, the extent of which remains at your sole discretion, and which may include, without limitation, the following Personal Data:

- **Identification and contact data:** Surname, first name, date and place of birth, nationality, postal address, email address, telephone number;
- **Data relating to financial securities:** Number of shares or units, transaction history, amounts invested, subscription price, ownership percentages;
- **Legal and governance documents:** Subscription forms, shareholders' agreements, minutes of general meetings, corporate decisions;
- **Navigation and connection data:** IP addresses, login credentials, activity logs on the platform.

Sensitive data transferred and restrictions or safeguards applied

The Parties do not anticipate the transfer of special categories of data (sensitive data). The processing of such data is limited to the mutually agreed safeguards and in accordance with applicable law.

Frequency of the transfer

The transfer takes place on a continuous basis throughout your use of the Subscription Services.

Nature of the processing

Your Personal Data will be processed in accordance with the Terms (including this Agreement) and may be subject to the following activities:

1. Storage, hosting and organisation of the data on our platform;
2. Automatic calculation of capitalisation tables and generation of documents (e.g. share transfer registers);
3. Provision of communication tools between You and your shareholders;
4. Operations necessary to ensure the security and improvement of the Subscription Services.

Purpose of the transfer and further processing

We will process your Personal Data to the extent necessary to provide the Subscription Services in accordance with the Terms, as specified in the Order Form, and as instructed by You in your use of the Subscription Services.

Retention period of Personal Data

Subject to the "Deletion or return of Personal Data" section of this Agreement, We will process your Personal Data for the term of this Agreement, unless there is a legal retention obligation (in particular for compliance with company law regarding the traceability of financial securities).

Appendix 2: Sub-processors

To help provide our Subscription Service, We engage Sub-processors for our data processing activities. A list of Sub-processors and the reasons why We use their services can be found in our **Privacy Policy**.

Appendix 3: Quality charter

We undertake to comply with the Quality Charter, and in particular the following points, which guarantee the quality of our service:

1. Ensuring the availability of your data:

Data hosting:

We host all your data, including backups, in data centres located in France.

We replicate the data across several data centres to ensure its durability and availability in the event of a disaster.

Data backups:

The database is also backed up and tested daily, together with a backup restoration process.

We continuously replicate all data on two nodes for databases, and three nodes for storage on AWS S3.

Each node is hosted in a specific data centre, geographically separate from the others.

In the event of an incident in a data centre, the data stored there is automatically replicated to the other data centres.

2. Guaranteeing the integrity of your data:

Securing access:

We require all users of the Application to authenticate with a personal email and password, subject to a strict password policy.

We log all logins and login attempts in order to detect any fraudulent use of the Application.

We ensure internally that access to data is restricted to duly authorised employees, via a VPN.

Traceability of system access and data modifications:

We implement audit logs to identify and archive all access to systems, as well as all access to and modifications of data on those systems.

We also ensure that all technical system events, such as errors, are identified and archived separately.

Logs are automatically replicated three times across three remote data centres in France (AWS servers, ISO 27001 certified), with automatic failover from one to another in the event of an incident.

Finally, audit logs are retained for one year.

3. Preserving the security of your data

Securing IT equipment:

We implement several measures to secure our IT equipment, including:

- Automatic session locking
- Disk encryption
- Anti-virus protection
- Firewalls

Securing the network and the database:

We also work to secure our network and our database.

To this end, We use VPN solutions to ensure an encrypted and secure connection to the network and enhanced data protection.

We also require complex passwords that must be changed periodically.

Finally, We ensure strict separation of development, test and production environments.

Securing the code:

In addition to securing our IT equipment, network and database, We work on securing our code.

To this end, We have implemented strict access control to the source code, with systematic peer review when merging new code.

We also ensure centralised management of rights across all Software-as-a-Service tools.

Finally, We regularly train our employees and run awareness campaigns on data confidentiality and security.

4. Guaranteeing the confidentiality of your data

Awareness and accountability of our teams:

We carry out systematic background checks on candidates.

We also require all our team members to sign a confidentiality agreement and adhere to our security and confidentiality charter.

Finally, We limit access to your data to team members who have a need to access it in light of their role.

Data encryption:

All data, including backups, is encrypted both in transit and at rest (AES-256 algorithm).

Any sensitive data that may be processed is systematically anonymised.