Data privacy policy (summary)

(The French version prevails)

1. Preamble and main definitions

The purpose of this policy is to describe the process for managing personal data (personal data) within ABC arbitrage Group in accordance with European and French regulations on personal data.

"Personal Data" means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity;

"Sensitive data": refers to 3 types of data, namely: (i) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, (ii) data on health or sexuality, (iii) data linked to offences, convictions or security measures, Unique national identification number (NIR for France) ;

"Data subject": means any person to whom personal data relate, identified or identifiable directly or indirectly ;

"Processing of Personal Data" means any operation or group of operations applied to Personal Data, regardless of the online service medium and the process used.

2. Scope

This policy applies to all data subjects and to any Group company directly responsible for processing personal data on their behalf or on behalf of any customer or any other Group company. This policy and the good practices detailed in it also serve as a reference for Group companies that are not formally subject to the obligations arising from the EU General Data Protection Regulation (GDPR).

The group applies any local specificities resulting from existing local constraints.

The principles described in this policy also apply, where relevant, to the Group's service providers, suppliers, and partners who have access to or process Personal Data on its behalf.

3. Personal data protection commitments

ABC ARBITRAGE, a public limited company with a Board of Directors, registered in the Paris Trade and Companies Register under number 400 343 182, whose registered office is located at 18, rue du Quatre Septembre 75002 Paris, is the data controller.

As the controller of Personal Data, the Group ensures that the Personal Data entrusted to it is protected, confidential, unaltered, available and secure. It takes all necessary measures to provide clear and transparent information on the collection and processing of such data, and ensures that the necessary technical and organizational measures are in place to protect them and ensure that their processing complies with applicable regulations. The Group's Legal Department is responsible for overseeing matters related to the protection of personal data, while compliance with the GDPR is ensured jointly by the Legal Department and the Head of Compliance and Internal Control (RCCI).

Personal data containing sensitive data will be processed in very limited cases, and under strict conditions (consent of the individual, data already in the public domain, processing essential to legal action or explicitly authorized by national legislation).

In the event of a substantial change to this Privacy Policy, the Group undertakes to notify the individuals concerned through appropriate channels (for example, via its website or by direct communication, where applicable).

4. Collection of personal data: purposes, recipients and principles

In the course of providing its services or complying with its legal obligations, the Group may need to collect Personal Data, for example, to manage a contractual relationship, job applications, litigation, comply with its legal and regulatory obligations, prevent fraud,

monitor share ownership, gain access to premises and information systems, and so on. In certain cases, the deletion of Personal Data may make it impossible for the Group to continue to perform the contract or meet its legal obligations.

The recipients of Personal Data are Group companies, partners and supervisory authorities. Any disclosure of Personal Data to third parties (private or public entities) is limited to cases necessary for the fulfillment of legal, regulatory, or contractual obligations. The Group ensures that these third parties provide appropriate safeguards for the protection of personal data and that such transfers are governed by contractual agreements.

Personal data is processed in accordance with the following essential principles:

- **Purpose:** before any processing of personal data, a purpose must be determined.
- **Legal basis:** the processing of personal data must have a legal basis (application of a legal obligation or contract). If this is not the case, there must be a legitimate interest that does not infringe privacy.
- **Explicit consent (opt-in):** When the processing is based on the data subject's consent, such consent is obtained explicitly, freely, specifically, and with full understanding prior to any collection or processing of Personal Data. The data subject may withdraw their consent at any time.
- **Minimization of personal data:** the collection of personal data must be strictly necessary for the specified purpose.
- **Quality of personal data**: personal data must be accurate and up-to-date throughout its life cycle.
- **Personal data retention periods**: personal data must not be kept longer than is necessary for the purpose for which it is to be used. These periods are established upstream and for the whole group, according to the different types of data and purposes.
- **Security measures**: security measures are in place to protect personal data, notably via the Information System.
- **Subcontracting:** In order to ensure the protection of Personal Data and respect for the rights of third-party recipients, the Group implements the necessary security measures with any subcontractors, notably via a written contract and a specific confidentiality agreement. The subcontractor must provide appropriate technical and organizational guarantees and process the data in accordance with the principles listed above.

5. Droits des personnes concernées

In order to control the use of Personal Data, data subjects have the following rights:

- **the right to object** to the processing of Personal Data;
- **the right to information** on the use of Personal Data;
- **the right to access and obtain information** on the data held and how it is processed;
- **the right to rectification** of inaccurate or incomplete Personal Data;
- **the right to erase** personal data in certain circumstances;

- **right to portability**: in certain circumstances and only for personal data supplied directly to any Group company;
- **the right to limit** the processing of personal data;
- **the right to define directives** concerning the conservation, erasure and communication of Personal Data after the death of the data subject;
- **the right to lodge a complaint** with the national supervisory authority;
- **the right to withdraw consent** to the processing of Personal Data.

These rights may be exercised by sending an e-mail, together with a copy of an identity document (national identity card or passport), to gdpr@abc-arbitrage.com. Details of these rights can also be obtained by contacting the same address. A reply will be provided as soon as possible.

6. Personal data security measures

Each Group company implements appropriate organizational and technical security measures to protect Personal Data against malicious intrusion, loss, alteration or disclosure to unauthorized third parties.

Access to personal data is restricted to Group employees or service providers acting on its behalf, who require it in the course of their duties. They are bound by a duty of confidentiality, and may be subject to disciplinary measures (ranging from a reprimand to dismissal for misconduct) if they fail to comply with the obligations and principles described in this policy. The Group has a zero-tolerance policy regarding violations of obligations related to the protection of personal data. All employees are encouraged to exercise caution to prevent unauthorized access to their personal data, including on digital equipment, in accordance with the information system usage charter appended to the internal rules. A presentation on the management of Personal Data is shared with all employees every year, and reminders are regularly sent to them.

Transfers of personal data within or outside the European Economic Area are subject to the same provisions.

7. Registering and archiving

The Group, or any of its subcontractors, undertakes to keep an up-to-date Register and will be responsible for ensuring that any new processing of Personal Data is recorded with the relevant information (name and contact details of the data controller, purposes of the processing, categories of data subjects and personal data, recipients of personal data, appropriate safeguards, planned deadlines for data erasure, general description of technical and organizational security measures).

The process of archiving personal data stored within the Group is subject to a specific procedure, access to which is restricted to network administrators, in order to comply with European and French regulations on personal data.

8. Cooperation with the authorities

The Group undertakes to maintain good relations with the *Commission Nationale de l'Informatique et des Libertés* (CNIL) or any other personal data protection authority. To this end, it will cooperate with and agree to be audited by the CNIL and to follow its advice on matters of which the CNIL may become aware.

9. Audit

Risks relating to the processing of personal data are identified and formalized in the Group's risk map. Issues related to their protection are thus incorporated into the Group's overall risk management and compliance framework.

The Group has included in its second line of defense program the assessment of compliance with archiving and personal data management constraints. Periodic checks on information systems may also include these points. Regular internal audits are conducted to verify that the Group's practices comply with this policy and applicable regulatory requirements.

10. Personal data breaches

If a breach of Personal Data is detected, a specific procedure will be applied, with the following steps:

1. Identification of a possible Personal Data breach
2. Creation of an "incident report form" and notification of senior management
3. Analysis of the incident to assess its impact
4. Communication of the incident to stakeholders
5. Management of communications to affected parties
6. Notification to the supervisory authority within 72 hours of detection
7. Confirmation that the request for deletion of disclosed data has been taken into account
8. Closure of the "incident report form".
9. Drafting of an incident report and identification of remediation actions.

11. Whistleblower system

An anonymous whistle-blowing system has been set up to enable employees and third parties to report any suspicion of corruption without risk of reprisal. Any person who deems it necessary can send an alert via the e-mail address lanceurdalerteabc@gmail.com or by post to 18 Rue du 4 septembre, 75002 Paris. He/she will be informed as soon as possible that the alert has been received, of the reasonable and foreseeable time required to examine its admissibility, and of the procedures for following up the alert. In the case of anonymous mail, no confirmation of receipt or information on the action taken will be sent to the sender. Reports are handled according to a formalized procedure, ensuring that they are reviewed and followed up on, and that appropriate

corrective or disciplinary measures are taken in the event of a confirmed violation. Full details are available in the dedicated public procedure.