- ANNEX I -
DATA PROTECTION

The personal data of both the informant (in the event that he/she discloses his/her identity) and the reported person obtained in the course of a report and any subsequent internal investigation will be processed by JB Capital Markets, S.V., S.A.U. ("JB Capital") and the companies of the Group, as co-responsible for the processing.

The sole purposes of this data processing are (i) to assess the complaints or information received through the Whistleblower Reporting Channel, (ii) to carry out the necessary internal investigations in accordance with the Internal Investigations Protocol, and (iii) to record the operation and effectiveness of JB Capital's Whistleblower Reporting Channel and the Criminal Risk Prevention Model.

The legal basis for the processing of data received as a result of a complaint or as part of a subsequent internal investigation is Article 6(1)(c) of the General Data Protection Regulation (EU) 2016/679. This means that the processing is necessary for the fulfilment of the legal obligation to have a Whistleblower Reporting Channel.

Personal data or any other information received through the Whistleblower Reporting Channel will be accessible only by the following persons or groups, and subject to the limitations established in each case:

(a) The members of the System Manager.

(b) The persons from the Compliance Department that the Compliance Director expressly designates with the capacity to manage the Whistleblower Reporting Channel, who undertake to comply faithfully with data protection regulations and with the duties of confidentiality in the management of the Channel.

(c) The professionals (internal and external) involved in the internal investigation and, where appropriate, the public authorities to whom the outcome of any internal investigation (investigating judge, public prosecutor or relevant administrative authority) may be transferred in the context of a criminal, disciplinary or disciplinary investigation.

(d) The human resources manager, only when disciplinary measures may be taken against an employee.

(e) The head of the legal services of the Company and of the Group, in the cases provided for in the Whistleblower Reporting Channel policy, and if appropriate, the adoption of legal measures in relation to the facts described in the complaint.

(f) The persons in charge of processing that may be appointed.

(g) The Data Protection Officer.

One of the Group's entities, JB Capital Management LLP, is based in the United Kingdom. Therefore, international transfers of data to the UK may occur when a complaint involves this entity or when this entity has to participate in the investigation process arising from the complaint. These potential international transfers are legitimate, as the United Kingdom is considered a secure territory in accordance with the Adequacy Decision issued by the European Commission on 28 June 2021. In addition, JB Capital also has third party providers located outside the European Economic Area, which may have access to personal data for the provision of services to JB Capital. In particular, Microsoft Corporation based in the USA, which provides the Outlook e-mail service, and Bloomberg, L.P., also based in the USA, which provides telephone recording and storage services. These international transfers are lawful, respectively, because they are based on Standard Contractual Clauses approved by the European Commission, and because they are based on a contract of standard data protection clauses adopted by a supervisory authority and approved by the European Commission. You can request more information about the protection measures implemented at the following email address: canaldenuncias@jbcapital.com and/or lopd@jbcapital.com.

Personal data subjects may exercise, in accordance with data protection legislation, their rights of access, rectification, deletion, opposition, limitation of processing and portability of their data, where applicable under the applicable regulations, by sending an e-mail to the address canaldenuncias@jbcapital.com. In addition, they also have the possibility of lodging a complaint with the relevant supervisory authority. In this case, the Spanish Data Protection Agency (www.aepd.es).

However, the exercise of such rights does not apply when the exercise of these rights is planned in relation to a complaint related to the prevention of money laundering and terrorist financing, in which case the provisions of article 32 of Law 10/2010, of 28 April, shall apply. In addition, in the event that the person to whom the facts described in the complaint refer exercises the right to object, it shall be presumed that, unless there is evidence to the contrary, there are compelling legitimate reasons that legitimise the processing of his or her personal data.

The identity and personal data of informants shall be confidential and shall not be communicated to the reported persons or to third parties, including in the case where the reported person exercises his/her right of access to his/her personal data. In this case, the reported person shall be denied access to the specific information on the identity of the informant.

Reports shall not contain excessive data or data that are not necessary for reporting the event in question. In the event that the report is found to contain excessive, useless or special category data, it shall be deleted immediately, without registration.

The personal data obtained as a result of the reports will be kept in the database of the Whistleblower Reporting Channel only for the time necessary to decide on the

appropriateness of initiating an investigation into the reported facts, and for a maximum of three months, unless it is necessary to provide evidence of the functioning of the Whistleblower Reporting Channel and the Criminal Risk Prevention Model. On the other hand, reports that have not been followed up can only be kept in an anonymised form (i.e. no individual can be identified as a party to the report or file).

Once the three-month period has elapsed, the data may continue to be processed outside the Whistleblower Reporting Channel, for the development of the investigation of the reported facts, or when necessary for the execution of civil, criminal, labour, administrative, disciplinary or any other type of action. Once the investigation has been completed, the data shall be kept in the logbook for a maximum period of 10 years.