GUIDELINES ON ANTITRUST, CONFLICTS OF INTEREST, MARKET ABUSE AND PRIVACY

SUMMARY DOCUMENT

Index

Introduction

Cassa Depositi e Prestiti S.p.A. (hereinafter, "**CDP**" or the "**Company**") places specific emphasis on risk management related to non-compliance with regulations, firmly believing that the adherence to laws and relevant regulations is an essential cornerstone in conducting its activities.

To this end, the current document - in line with the internal regulations approved by CDP's competent bodies - summarizes the guidelines and key measures adopted by the Company in the following areas of paramount interest, considering its operational activities:

- **Antitrust**
- **Conflicts of Interest**
- **Market Abuse**
- **Privacy**

Antitrust Guidelines

The Antitrust regulation aims to safeguard competition in the market by preventing companies from colluding or abusing their dominant positions, or in any way distorting competition to the detriment of competitors, suppliers, customers, and consumers. Furthermore, this regulation is designed to prevent concentration from reducing or eliminating competition in the market, and for this purpose, they provide for a prior review of such transactions.

Consumer protection regulations, on the other hand, aim to prevent professionals from engaging in unfair commercial practices to the detriment of consumers, which can, in turn, result in deceptive or aggressive commercial practices.

The CDP Group operates in the market in compliance with the Antitrust regulation and those for consumer protection, fully adhering to the principles of legality and integrity. Special attention is given to relationships with competitors, suppliers, customers, and other third parties.

To this end, the CDP Group has adopted an "Antitrust Compliance" Policy that outlines:

1) the guiding principles to inspire behaviors in order to promote a culture of compliance with Antitrust regulation and consumer protection regulations, with the aim of mitigating the risk of potential misconducts in line with the provisions of CDP's Code of Ethics;
2) the set of control measures implemented by CDP and its Group companies to ensure proper Antitrust risk management;
3) awareness initiatives regarding compliance with Antitrust regulation undertaken by the Parent Company and Group companies towards their subsidiaries.

CDP and the Group companies place a significant emphasis on their relationships with competitors, customers, suppliers, contractors, and third parties, with particular reference to:

a) Prohibition of anti-competitive agreements:

In the context of their relationships with competitors, CDP and the Group companies:

- do not enter into agreements of any kind concerning the commercial policy to be adopted in the market (*e.g.*, sales conditions, commercial policy, applied prices, etc.);
- refrain from cooperating with competitors in public tenders to coordinate their participation strategies;
- do not exchange Sensitive Information with competitors capable of reducing uncertainty about a competitor's current or future behavior in the market. In the event that Sensitive Information is received from competitors, it is essential to immediately and explicitly oppose any further disclosure, clarifying that CDP and/or the Group companies will not use it in determining their commercial policy ("Opposition to Exchange");
- do not exchange Sensitive Information during meetings and/or gatherings organized by trade associations.

b) Relationships with customers and suppliers: Prohibition of Vertical Agreements

CDP and the Group companies refrain from negotiating with suppliers and/or customers the resale price of products or services purchased by CDP and the Group companies. They also refrain from:

- receiving or providing incentives related to the application by customers of CDP and the Group companies of a recommended resale price;
- restricting the ability of CDP's and/or the Group companies' customers to resell products (or provide services) in certain territories and/or to certain customers;
- restricting the ability of CDP's and/or the Group companies' customers to resell products (or provide services) via the internet.

c) Prohibition of Abuse of Dominant Position

In order to ensure compliance with Antitrust regulation, it is necessary that, if CDP or any company within the Group assumes a dominant position, they refrain from:

- imposing on their customers purchase prices, selling prices, and other transaction conditions that are unfair (*e.g.*, charging prices higher than those that would be allowed in a competitive market);
- imposing exclusive procurement obligations on customers to deal exclusively with the dominant entity;
- imposing on customers the obligation to report any more advantageous offers received from other suppliers to the dominant entity and accepting such offers only if the dominant entity decides not to offer equivalent conditions (so-called English clause);
- conditioning the sale of a particular product or service on the purchase of another unrelated product or service that would otherwise be sold separately (tying or bundling);
- offering discounts aimed at customer loyalty (*e.g.*, with annual targets or by applying retroactive discounts);
- unjustifiably refusing to provide intermediate products or access to essential infrastructure to customers or competitors, which is necessary to compete in one or more downstream markets.

d) Concentrations

In case of CDP or a Group company intends to participate in a concentration that exceeds the turnover thresholds prescribed by the Antitrust regulations, the relevant organizational unit of CDP and the Group company, with the support of the relevant corporate functions, shall proceed to notify the Antitrust Authority. In case of corporate transactions such as acquisitions, mergers, establishment of joint ventures, transfer or sale of business units, or assets with attributable turnover, the relevant organizational unit of CDP or the Group company shall inform the relevant corporate functions in order to assess whether the operation is likely (i) to be classified as a concentration and, if so, (ii) to exceed the notification thresholds prescribed by the Antitrust regulation and any relevant international merger control regulations for the purpose of the transaction.

e) Unfair Business Practices

To ensure compliance with consumer rights protection regulations, it is necessary for the organizational units of CDP and Group companies, in case of dealings with consumer clients:

- pay special attention to include in pre-contractual and contractual documents signed by clients clear and visible information regarding: (i) the terms of the advertised product/service, (ii) its duration, (iii) the associated costs, and (iv) any withdrawal procedures;
- inform the consumer, in the case of joint packages involving multiple products issued by CDP and/or Group companies, about: (i) the types of services offered, (ii) constraints related to joint purchases, and (iii) any withdrawal procedures;
- refrain from advertising savings product promotions by indicating certain yields as guaranteed when they can only be obtained under complex conditions that are difficult to monitor without a real guarantee on the invested and tied-up capital;
- refrain from promoting the application of a particularly favorable promotional interest rate without indicating: (i) the time limitations of the promotion and (ii) the interest rate applied at the end of the promotional period.

f) Greenwashing Practices

CDP and Group companies refrain from engaging in greenwashing practices, and to that end, with reference to all types of products and services offered that aim to achieve environmental, social, and governance ("ESG") objectives, they ensure that:

- ESG objectives and risks underlying various initiatives are clearly defined and identified during the product/service ideation phase;
- ESG purposes are accurately and clearly represented in pre-contractual, contractual, and advertising documentation related to such products;
- internally, appropriate monitoring mechanisms are activated to ensure that the ESG objectives underlying various initiatives are consistently upheld over time and demonstrable to third parties;
- adequate information is provided to customers, as contractually required, regarding compliance with ESG commitments.

Conflicts of interest Guidelines

The increasing activities of financial operators and the diversification of services they offer can lead to potential conflicts of interest. For this reason, regulations and reference best practices, recognizing that intermediaries cannot completely eliminate conflicts of interest, require them to correctly identify and manage conflicts of interest to prevent them from adversely affecting the interests of clients or the Company.

To this end, operators are required to develop and maintain a company policy for managing conflicts of interest that is appropriate to the size and complexity of their activities (the so-called proportionality criterion). In light of the above, CDP has adopted a Regulation that formalizes the measures voluntarily taken by the Company and establishes the rules that CDP employees must follow to ensure the maximum management of situations that could generate potential conflicts of interest, taking into account the aforementioned principle of proportionality.

Periodically or upon specific request, potential conflict situations arising from the business activities or transactions carried out by CDP are internally documented. The mapping phase of potential conflicts of interest involves identifying circumstances that could give rise to conflicts (even potential ones), including: (i) between CDP or one of its employees on one side, and CDP's clients on the other side, at the time of the execution of any transaction/activity or a combination of transactions/activities directly provided by CDP; or (ii) between CDP and one of its employees who has decision-making authority over any transaction in which CDP is involved or participates, where such employee has (directly or indirectly) an interest of any kind in the transaction. For the purpose of mapping potentially detrimental conflicts, the following circumstances are relevant, among others:

1. when from the execution or omission of a transaction/activity with a specific client, CDP or one of its employees could obtain significant benefits, financial gain, or avoid financial loss, all to the detriment or at the expense of the client;
2. when CDP or one of its employees has a benefit of any kind (even non-financial) in favoring the interests of one client rather than another;
3. when CDP or one of its employees receives or could receive an incentive - in the form of money, goods, or services - to favor the interests of specific clients;
4. the execution of a transaction/activity by CDP with a specific client without adequate objective reasons;
5. the existence of a distinct or potentially conflicting interest for CDP or one of its employees in the transaction compared to the client's interest;
6. the existence of an interest - both personally and for a close family member - of a CDP employee actively participating in any phase of a transaction, where the impartial and objective exercise of their functions is compromised by family, emotional reasons, or economic interests.

In the conflict of interest mapping, for each scenario listed by way of example and not exhaustively, a set of mitigation measures is highlighted. These measures should be considered as minimum safeguards. If a single transaction/activity falls under multiple conflict scenarios, the mitigation measures identified in the mapping should be considered collectively.

The identification of conflicts of interest and the subsequent assessment of measures (as described in the Mapping), in place for their management, may undergo updates in response to organizational changes (*e.g.*, changes in the organizational structure, including changes in the ownership structure of CDP or the Group), regulatory changes, or changes in the participatory structure/business model of the Group (*e.g.*, acquisition of new companies, changes in the operational scope of one of the Group's companies). Additionally, employees responsible for business activities, as well as the respective heads of these units, are required, within their respective areas of competence and within their activity, to identify, based on the elements outlined in the previous paragraph, further situations of potential conflicts of interest that may arise during their activities and to promptly communicate them to Compliance.

Based on the principles outlined in the Regulation adopted by CDP regarding conflicts of interest, the competent structures, upon identifying a potential conflict of interest situation, conduct the necessary investigations, including involving the Compliance Function, to identify any measures required by the Mapping that should be adopted. Following this, CDP's decision-making body, with specific reference to the transaction subject to the potential conflict and prior to its approval, may:

1) proceed with the transaction (so-called conflict of interest management), deeming the organizational and/or operational measures identified in the previous paragraph to be sufficient and having implemented these measures as indicated in the Mapping;
2) proceed with the transaction, provided that specific client disclosure is also provided before the conclusion of the transaction, highlighting the nature and/or source of the conflict of interest;
3) abstain from carrying out the transaction if it is seriously affected by a conflict situation. This last option should be used as a last resort when there is no certainty that the identified conflict of interest situation can be adequately managed, and therefore, when it is not possible to guarantee to the client that the risk of harm is avoided.

Market Abuse Guidelines

CDP has adopted an internal regulation to outline and define the circumstances that are relevant for CDP's compliance with Italian and European regulations concerning Market Abuse. The regulation has been adopted by CDP as an issuer of financial instruments listed on regulated markets or multilateral trading systems in Italy or other EU Countries, as well as due to transactions that may grant access to insider information, even from third-party issuers.

In particular, the regulation establishes the general framework by identifying the regulatory aspects relevant to CDP, as well as specifying the general measures that have been detailed in specific operational regulations in the following areas:

1) Abuse and/or Unlawful Communication of Insider Information

Those subject to compliance with the Market Abuse Regulation are not allowed to: (i) abuse or attempt to abuse Insider Information; (ii) recommend others to abuse Insider Information or induce others to abuse it; (iii) unlawfully communicate Insider Information.

For this purpose, CDP has implemented an internal process for the identification, management, internal communication, and storing of Confidential and Insider Information. Specifically, CDP has defined:

- the internal procedure for qualifying and identifying Confidential and Insider Information;
- operational methods for managing and internally disseminating information, both in paper and electronic formats;
- internal organizational measures to ensure confidentiality (*e.g.*, dedicated working teams, Chinese walls);
- appropriate behaviors to be adopted in the operational process of managing Confidential and Insider Information;
- obligations and prohibitions to be observed in accessing, directly and indirectly, the trading of financial instruments to which the information relates;
- controls to mitigate the risk of unlawful activities being carried out.

2) Public Disclosure of Insider Information

To ensure compliance with the obligation to publicly disclose Insider Information directly concerning it, CDP has established, through a specific operational regulation:

- roles and responsibilities, methods, and tools for identifying and segregating Relevant Information;
- roles and responsibilities, methods, and tools for identifying, segregating, and disseminating Insider Information that allows rapid access and comprehensive, accurate, and timely evaluation of information by the public;
- decision-making process and procedures for managing any delays in the public disclosure of Insider Information;
- procedures for verifying the existence of necessary conditions to delay the disclosure of Insider Information to the market, and related formalization;
- organizational measures to ensure the confidentiality of Insider Information if a decision is made to delay

disclosure;

- methods and timelines for notifications to the Supervisory Authority as required by applicable regulations.

3) Insider List and Relevant Information List

CDP has defined, through a specific operational regulation:

- roles and responsibilities for the management and updating of the Insider List and the Relevant Information List ("RIL"), identifying the person responsible for maintaining these lists (the "List Manager");
- layout, format, and content of the Insider List and the RIL;
- operational procedures for maintaining and managing the Insider List and the RIL;
- information flows aimed at ensuring the proper maintenance and updating of the Insider List and the RIL;
- criteria for identifying individuals to be included/removed and for updating the data;
- obligations of individuals listed on the Insider List and the RIL;
- methods of communication with/from individuals listed on the Insider List and the RIL;
- access requirements to the content of the Insider List and the RIL to ensure confidentiality;
- requirements for the storage and archiving of data registered into the Insider List and the RIL.

4) Execution or Receipt of Market Soundings

In order to ensure compliance with the obligations related to the execution or receipt of market soundings, CDP, through the adoption of a specific regulation, has:

- defined the operational rules to be followed in situations involving the execution and receipt of market soundings;
- identified the operational tools for collecting and preserving the information required by the relevant regulations;
- established the conduct rules to be implemented to ensure the proper management of the flow of Insider Information provided or received during the market sounding, with the aim of preventing the abuse and improper communication of Insider Information.

5) Internal Dealing

In order to ensure compliance with obligations related to internal dealing, CDP has defined, through a specific regulation:

- the scope of so-called "Relevant Persons";
- the obligations and prohibitions that Relevant Persons are required to observe;
- roles and responsibilities for the initial census and ongoing updates of Relevant Persons and the transactions they notify;
- controls to mitigate the risk of unlawful activities being carried out.

Privacy Guidelines

Since May 25, 2018, the EU Regulation 2016/679, known as GDPR (“General Data Protection Regulation”), became fully applicable in all Member States. GDPR pertains to the protection of individuals with regard to the processing and free movement of personal data.

GDPR was introduced to address the need for legal certainty, harmonization, and simplification of rules governing the transfer of personal data from the EU to other parts of the world. It also serves as a response to challenges posed by technological advancements and new economic growth models, taking into consideration the increasing need to protect personal data as perceived by the EU citizens.

CDP considers the protection of personal data of its clients, employees, and suppliers as an obligation that goes beyond mere regulatory compliance. For this reason, it has established specific policies and procedures aimed at defining roles and responsibilities, internal rules, and methodologies to ensure the management and mitigation of risks to the rights and freedoms of individuals associated with the processing of personal data.

In particular, the "Group Policy Guidelines on the Processing of Personal Data" and the related internal procedures specify roles and responsibilities, along with operational methods, aimed at fulfilling obligations related to personal data protection (including the implementation of key changes introduced by GDPR):

1) managing personal data breaches (known as "data breaches"); In particular, it is mandatory for CDP, within 72 hours from the moment it becomes aware of a personal data breach, to send a communication to the Data Protection Authority (“*Garante*”) containing at least the following elements: a) the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records concerned; b) the name and contact details of the Data Protection Officer (DPO) or another contact point where more information can be obtained; c) the potential consequences of the personal data breach; d) the measures taken or proposed to be taken by the Data Controller to address the personal data breach and, if applicable, to mitigate its potential negative effects. The process for managing personal data breaches is structured as follows: 1. Anomaly Detection: Detection of an anomaly by the relevant organizational units; 2. Qualification of the Breach: Initial analysis of the anomaly aimed at confirming or ruling out the presence of a breach; 3. Assessment of Causes and Impacts of the Incident: Analysis of the causes that led to the breach, evaluation of the potential impacts on the confidentiality, integrity, and availability of personal data, and identification of countermeasures to address it; 4. Notification of the Breach: Sending of information related to the personal data breach to the Data Protection Authority and, if required, to the data subjects concerned; 5. Archiving: Collection and archiving of all documentation related to the management of the breach and updating of the "data breach" inventory in compliance with applicable regulations.;
2) formalizing the privacy impact assessment ("Data Privacy Impact Assessment");
3) preparing and updating the Register of Processing Activities;
4) appointing and managing external Data Processors through the signing of a formal agreement that outlines the responsibilities of the Data Processor, and specifically: • Personal data subject to the contract must only be processed upon documented instruction from the Data Controller; • Persons authorized to process personal data must commit to confidentiality; • All measures required under Article 32 of the GDPR must be implemented; • Assist the Data Controller with appropriate technical and organizational

measures, to the extent possible, in responding to data subject requests to exercise their rights; • Assist the Data Controller in ensuring compliance with the obligations imposed by current regulations, taking into account the nature of the processing and the information available to the external Data Processor; • Promptly report any breaches of personal data to the Data Controller in accordance with the GDPR and actively cooperate with the Data Controller to fulfill the obligations set out in Articles 33 and 34 of the GDPR; • Upon the Data Controller's request, delete or return all personal data once the provision of the service/activity has ended and delete any existing copies, unless EU law or Member State law requires data retention; • Provide the Data Controller with all necessary information to demonstrate compliance with the obligations set out in Article 28 of GDPR and cooperate, as necessary, with verification activities, including inspections, carried out by the Data Controller or another entity authorized by the Data Controller;

5) applying the principles outlined in the Article 5 of GDPR (*e.g.*, lawfulness, transparency, fairness, minimization, accuracy, etc.); in particular, with regard to the principles of lawfulness, transparency, and fairness, CDP considers that processing is lawful only if, and to the extent that, at least one of the following conditions applies: • The data subject has given consent to the processing of their personal data for one or more specific purposes; • Processing is necessary for the performance of a contract to which the data subject is a party or for the execution of pre-contractual measures requested by the data subject; • Processing is necessary to comply with a legal obligation to which the Data Controller is subject; • Processing is necessary to protect the vital interests of the data subject or of another natural person; • Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; • Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data. With regard to the limitation of purpose and data minimization, CDP ensures that data is collected for specified, explicit, and legitimate purposes and subsequently processed in a manner that is not incompatible with those purposes. Furthermore, CDP guarantees that the data subject to processing is adequate, relevant, and limited to what is necessary for the purposes for which it is processed (the principle of "data minimization" - Article 5, paragraph 1, letter c) of GDPR) and that it is accurate and, where necessary, kept up to date. Data is also stored in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (the principle of "storage limitation" - Article 5, paragraph 1, letter e) of GDPR) and is processed in a way that ensures its integrity and confidentiality, including protection against unauthorized access or use of personal data and the equipment used (the principle of "integrity and confidentiality" - Article 5, paragraph 1, letter f) of GDPR).

6) enabling data subjects to exercise their rights as specified in the Articles 15 – 22 of GDPR;

7) issuing notices and managing consent for data processing for specific purposes (*e.g.*, marketing, statistics, etc.).

Pursuant to the Article 32 of GDPR CDP has also implemented adequate technical and organizational measures to ensure an appropriate level of security in line with the risk. More specifically, CDP has established three different levels of control:

1) Governance: Organizational security measures that primarily involve the adoption and implementation of

policies and procedures.

2) Application Level: Technical and organizational security measures to be implemented to allow the proper governance of application systems in terms of user access, profiling, log tracking, and backup.

3) Infrastructure Level: Technical and organizational security measures related to data encryption, account management in operating systems, physical and logical segmentation of infrastructure components, patching, and tracking activities.

Lastly, it should be noted that CDP has appointed a Data Protection Officer in accordance with Articles 37, 38, and 39 of GDPR, with the following main responsibilities: i) informing and providing advice to various business functions on specific issues related to the processing of personal data; ii) monitoring compliance with EU and national regulations and CDP's internal policies; iii) validating the results of the data protection impact assessment and overseeing its progress; iv) cooperating with the Supervisory Authority and acting as the point of contact for matters related to data processing, and conducting consultations, if necessary, on any other issue.