**Disclosure on personal data processing**

Dear Sir or Madam,

Within the framework of its institutional purposes, in compliance with the EU Directive 2019/1937 transposed into our law by Legislative Decree no. 24. and in accordance with the obligations provided for by data processing regulations, CA Auto Bank S.p.A. intends to provide its employees, partners, customers, suppliers, consultants, collaborators (the "**Interested Party**" or collectively the "**Interested Parties**") with the specific information on the processing of personal data that is necessary in relation to reports sent through the Whistleblowing Portal (hereinafter the "**Whistleblowing Portal**" or the "**Portal**" for short). The Portal is accessible through a link available on the website of the Data Controller, pursuant to Art. 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 ("**GDPR**") and the European and national legislation that amends and/or supplements it ("**Applicable Privacy Legislation**"), including the provisions on the protection of personal data set forth in Legislative Decree No. 196/2003, as renewed by Legislative Decree No. 101/2018 (hereinafter "Privacy Code").

It should be noted that in case of non-anonymous reporting, CA Auto Bank guarantees that that the identity of the reporting person will be protected under any and all circumstances.

1) **Data Controller**

The Data Controller is CA Auto Bank S.p.A. ("**CA Auto Bank**"), headquartered in Turin, Corso Orbassano, 367.

In using the personal data that you have provided as a reporting person, CA Auto Bank also acts as a joint controller with its parent company, **Credit Agricole Consumer Finance S.A.**, and with **Credit Agricole S.A.**, parent company of the Crédit Agricole Banking Group. These companies have made available to CA Auto Bank the reporting tool and are responsible for receiving/managing the alert containing the subject of the report.

2) **Data Protection Officer**

For any direct contact - formal and urgent, other than the exercise of the rights provided in paragraph 10) - you may contact the Data Protection Officer by:

• Email: dpo-italia@ca-autobank.com.

3) **Categories of personal data**

The Joint Data Controllers will process the data provided by the reporting person to describe the alleged unlawful conduct of which he/she has become aware, committed by persons who interact with the Company in various capacities, in order to carry out the necessary investigative activities into the reported events and the adoption of the consequent measures.

The personal data collected and processed include vital data, contact data, in case the reporting person decides not to remain anonymous and access the Portal on a "confidential" basis, data relating to the

employment relationship, the position held, as well as the elements contained in the report (hereinafter "**Common Data**").

The Joint Data Controllers will only process data belonging to specific categories, i.e., data that may reveal, among other things, racial and ethnic origin, data relating to health and sexual life (the "**Specific Data**"), if you freely decide to provide them as distinguishing features of the report. In any case, Ca Auto Bank will process these data solely for purposes strictly related and conducive to the verification of the authenticity of the reports of irregularities or to the fulfillment of specific legal obligations (related to the purposes of the report).

Common Data and Specific Data are hereinafter collectively referred to as "**Personal Data**".

Unless they are relevant for the purpose of the report, judicial data (i.e., personal data related to criminal convictions and offenses or related security measures) should not be included. In any case, CA Auto Bank will process such data only for purposes strictly related and conducive to the verification of the authenticity of the irregularity reports or to the fulfillment of specific legal obligations (related to the purposes of the report).

The Personal Data will be provided directly by you by filling in the relevant fields when sending the report, or at a later date if you decide to provide additional elements to substantiate the report, through the Portal's messaging system, which allows you to establish a virtual conversation with the body in charge of handling the report.

The processing of personal data is governed by the principles of fairness, lawfulness and transparency and the protection of confidentiality and the rights of the reporting person, as well as the other principles set out in Article 5 of the GDPR.

**4) Purpose and legal basis of data processing**

Personal Data will be processed in order to handle your report and to take the appropriate and necessary measures for your protection on a strictly confidential basis.

In view of the above, the legal basis for processing the personal data provided is

a) the need for the Data Controller to comply with its legal obligations pursuant to art. 6 para. 1 (c) of the GDPR (see in particular Legislative Decree no. 24 of March 10, 2023 and article 6, para. 2 bis et seq. of Legislative Decree no. 231 of June 8, 2001, as amended by Law no. 179/2017 "Provisions on the administrative responsibility of legal persons, companies and associations, including those without legal personality") and the legitimate interest of the Data Controller pursuant to article 6, para.1(f) of the GDPR for reports not expressly contemplated by the legislation.
   With regard to the processing of specific categories of personal data, the legal basis is article 9, para. 2 (b) of the GDPR in the presence of the of the need for the Data Controller or the Data Subject to fulfill contractual obligations and to exercise specific rights in the field of labor and social security and social protection law, and article 9, para.2 (f) of the GDPR in the presence of the need to establish, exercise or defend a right when the judicial authorities exercise their judicial functions; and

b) the need to ascertain, exercise or defend a right in court, should it be necessary on the basis of the legitimate interest of the Data Controller, in accordance with Article 6, paragraph 1(f) of the GDPR.

**5) Manners of processing**

The processing of Personal Data will be carried out - in accordance with the principles of fairness, lawfulness and transparency - through computerized, manual and/or electronic media and/or tools, with a rationale strictly related to the purposes of the processing and in any case guaranteeing the confidentiality and security of the data and compliance with the specific obligations established by law.

The availability, management, access, storage and usability of the data are guaranteed through the adoption of technical and organizational measures to ensure an adequate level of security, in accordance with articles 25 and 32 of the GDPR.

The processing is carried out by persons specifically authorized by the Data Controller, in compliance with the provisions of article 29 of the GDPR.

**6) Retention periods**

The Personal Data will be retained for 12 (twelve) months from the date of notification of the final outcome of the reporting procedure, in compliance with the principle of minimization referred to in Article 5, paragraph 1 (c) of the GDPR, as well as the legal obligations to which the Data Controller is subject pursuant to article 14 of Legislative Decree No. 24 of March 10, 2023, implementing EU Directive 2019/1937.

In the event of legal disputes, the personal data will be kept for the duration of the dispute and until the time limits for appeals have expired.

For further information, please contact the Data Controller or the DPO using the contact details provided in 2) above.

**7) Recipients of Personal Data**

Your Personal Data will not be disclosed to third parties, except when such disclosure is required by law or by public authorities for the purposes of defense or security, or for the prevention, detection or investigation of criminal offenses.

In order to carry out its activities and for the purposes indicated in paragraph 4 above, the Data Controller may communicate your personal data to third parties, in compliance with the provisions of the Regulation and the aforementioned Privacy Code, such as:

- the provider of the Portal and related maintenance services, within the scope of its activity as system administrator, which acts as Data Processor pursuant to art. 28 of the GDPR;
- the joint controllers Credit Agricole Consumer Finance S.A. and Crédit Agricole S.A., limited to the persons in charge of the control functions;

- the competent authorities (e.g., institutions and/or public authorities; judicial authorities and law enforcement agencies) who make a formal request; in this case, the communication of the data is necessary to comply with a legal obligation.

Your Personal Data will not be transferred to countries outside the European Union or to international organizations.

## 8) Confidentiality and protection of the whistleblower

The Data Controller applies article 6 of Legislative Decree No. 231/2001, as amended by article 2 of Legislative Decree No. 179/2017, under the heading "Protection of the employee or collaborator who reports wrongdoing in the private sector", which provides for the protection of the confidentiality of the identity of the reporting person in the activities of handling the report and prohibits retaliation or discrimination, whether direct or indirect, against the reporting person for reasons directly or indirectly related to the report.

The Data Controller also applies the provisions of article 12 of Legislative Decree No. 24 of March 10, 2023, which transposes EU Directive 2019/1937, whereby the identity of the reporting person and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the reporting person, to persons other than those competent and authorized to receive or follow up on reports.

Therefore, within the limits set forth in the aforementioned article 12, and except in cases where

a) knowledge of the identity of the reporting person is absolutely necessary for the defense of the reporting person; or

b) there are mandatory provisions requiring the Data Controller to disclose the identity of the reporting person; or

c) there is liability for defamation under the provisions of the Criminal Code or article 2043 of the Civil Code, and in cases where confidentiality is not enforceable by law (e.g., criminal, tax or administrative investigations, inspections by supervisory bodies),

the identity of the reporting person will be protected, as soon as the report is received and at all stages thereafter, in accordance with the applicable provisions of the Privacy Code in force, and may not be disclosed, without the express consent of the reporting person, to persons other than those responsible for receiving or following up on the report who are authorized to process such data pursuant to articles 29 and 32(4) of the GDPR and article 2 quaterdecies of the Privacy Code.

All persons receiving and/or involved in the processing of reports are required to protect the confidentiality of such information.

## 9) Rights of the Data Subject

In accordance with articles 15 to 22 of the GDPR, you have the right to:

- obtain confirmation from the Data Controller as to whether personal data relating to you are being processed and, if so, to have access to such data and, where the data have not been obtained from the data subject, to have all available information regarding their origin;

- know the purposes of the processing, the categories of the data concerned, the recipients or categories of recipients to whom the data have been or will be communicated, the expected data retention period or the criteria used to determine this period;

- request the Data Controller to erase the data or to restrict the processing of data concerning you;

- object to the processing of the data, without prejudice to the right of the Data Controller to consider your request, which may not be accepted if there are compelling legitimate grounds for processing that override your interests, rights and freedoms;

- request data portability in cases provided for by law;

- lodge a complaint with a supervisory authority (Privacy Garante).

It should also be noted that, in accordance with article 2, paragraph 1 (f) of Legislative Decree 101/2018), the Data Controller guarantees the confidentiality of your identity.

Requests must be addressed in writing to the Data Controller or to the DPO, to the contacts detailed indicated above.

**10) Limitations on the rights of the reported person and other parties concerned**

The rights under articles 15 to 22 of the GDPR may not be exercised (with a request to the Data Controller or with a complaint under article 77 of the GDPR), if such exercise may result in an actual and concrete prejudice to the confidentiality of the identity of the reporting person (see article 2 of the Privacy Code and article 23 of the GDPR) and/or to the pursuit of the objectives of compliance with the legislation on reporting unlawful conduct.

In particular, the reported person is informed that the exercise of these rights:

• will be carried out in accordance with the provisions of the law or regulations governing the sector (including Legislative Decree 231/2001, as amended by Law No. 179/2017 and Legislative Decree No. 24 of March 10, 2023);

• may be delayed, restricted or excluded, to protect the confidentiality of the reporting person's identity, by means of a reasoned communication to the party concerned without undue delay, unless such communication could jeopardize the purpose of the restriction for the period of time and to the extent that this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the party concerned;

• where appropriate, in such cases, the rights of the party concerned may also be exercised by resorting to the Garante per la Protezione dei Dati Personali ("**Garante**") in the manner provided for by article 160 of the Privacy Code, in which case the Garante shall inform the party concerned that it has carried out all the necessary reviews or checks, as well as of the right of the party concerned to seek judicial review.

Therefore, the exercise of the rights of the reported person (including the right of access) may be exercised to the extent permitted by the applicable law. In particular, it is noted that the request will be analyzed by the competent bodies in order to reconcile the need to protect the rights of individuals with the need to combat and prevent violations of the rules of good governance or of the regulations in force on the subject.