PRIVACY INFORMATION NOTICE ON THE PROCESSING OF PERSONAL DATA FOR REPORTING ON BREACHES (*WHISTLEBLOWING*)

(*Pursuant to Article 13 of Regulation (EU) 2016/679*)

Pursuant to Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (*General Data Protection Regulation*, hereinafter "*GDPR*"), the personal data provided by the Whistleblower will be processed in compliance with the above-mentioned legislation and in accordance with the principles of fairness, lawfulness and transparency.

1. Data Controller and Data Protection Officer

The BFF Banking Group processes the personal data contained in the Whistleblowing reports as Joint Data Controllers, in accordance with Article 26 of the GDPR, as the purposes and means of the processing activities have been jointly determined, in the manner set out in the relevant corporate procedures. The Joint Data Controllers are:

- **BFF Bank S.p.A.**, with registered office in Viale Lodovico Scarampo, 15, 20148 Milan, Italy, who is the parent company of the BFF Banking Group;
- **BFF Finance Iberia S.A.**, with registered office in Paseo de la Castellana 81, 28046 Madrid, Spain;
- **BFF Bank S.p.A. Sucursal en Espana**, with registered office in Paseo de la Castellana 81, 28046 Madrid, Spain;
- **BFF Bank S.p.A. Sucursal em Portugal**, with registered office in Rua Barata Salgueiro nr. 37, 6º esq 1250-042, Lisbon, Portugal;
- **BFF Polska S.A.**, with registered office in ul. Kilińskiego, 66, 90-118 Łódź, Poland;
- **BFF Bank S.p.A. Spółka Akcyjna Oddział w Polsce**, with registered office in ul. Kilińskiego, 66, 90-118 Łódź, Poland;
- **BFF MEDFinance S.A.**, with registered office in ul. Kilińskiego, 66, 90-118 Łódź, Poland;
- **BFF Ceska Republika s.r.o.**, with registered office in Roztylská 1860/1, 148 00 Praha 4, Czech Republic;
- **BFF Central Europe s.r.o.**, with registered office in Mostová 2, 811 02 Bratislava, Slovakia;
- **BFF Bank S.p.A. Ελληνικό Υποκατάστημα**, with registered office in Pentelis Ave. 72, Chalandri. t.c.1523, Greece;
- **BFF Immobiliare S.r.l.**, with registered office in Viale Lodovico Scarampo, 15, 20148 Milan, Italy;
- **BFF Techlab S.r.l.**, with registered office in Via Carlo Zima, 4, 25121 Brescia, Italy

In compliance with the provisions of Article 37 of the GDPR, it has been appointed a Data Protection Officer (DPO) who may be reached via e-mail at the following address DPO@bff.com.

2. Categories of personal data, purpose of processing and legal basis

The personal data provided to describe the alleged unlawful conduct of which the Whistleblower has become aware by virtue of their relationship with an entity of the BFF Banking Group, committed by subjects who interact with it in various capacities, are processed for the purpose of carrying out the necessary investigative activities aimed at verifying the validity of the fact being reported, the information contained in the report and the adoption, where applicable, of the ensuing provisions.

The personal data will also be processed to fulfill requirements for the defense of rights in judicial, administrative, or extrajudicial proceedings and when disputes arise from the report. Only the information and documents necessary to support the investigation of the alleged misconduct should be attached within the report. In the pursuit of the stated purposes, the Joint Data Controllers may process common personal data such as first name, last name, job role, affiliation structure, and qualification.

The report should not contain special data under Article 9 of the GDPR (information capable of revealing racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership in parties, trade unions, associations or organizations of a religious, philosophical, political or trade union nature, as well as personal data capable of revealing health and sex life) or judicial data under Article 10 of the GDPR (personal data relating to criminal convictions and offenses or related security measures). Should the report contain those categories of personal data, whether referring to the Whistleblower or to third parties, they will be deleted unless there are obligations to retain them or they are cases authorized by law or by the competent Data Protection Authority.

Personal data that are manifestly not useful for the processing of the report shall not be collected or, if accidentally collected, shall be deleted immediately.

The legal basis that legitimizes the processing of personal data is the fulfillment of a legal obligation to which a data controller is subject (Article 6, paragraph 1, lett. c) of the GDPR), specifically consisting of provisions regarding the protection of persons who report violations of national regulatory provisions.

3. Scope of communication and extra-EU transfer of personal data

Personal data collected from the report may be disclosed to the relevant Supervisory or Judicial Authority, if necessary.

After informing the Whistleblower, the final report of the Head of the Reporting System may be sent to:

- the Head of Group Human Resources & Organizational Development of BFF Bank S.p.A., for the activation of the disciplinary system;
- other corporate functions of the Bank, as well as the branches/subsidiaries affected by the facts described in the report, regarding any necessary measures to bring the 231 Compliance Management System and corporate procedures into compliance, while always maintaining the confidentiality obligations required by law.

However, the Head of the Breach Reporting System may forward the final report to other parties in the following cases governed by the procedure:

- to the Chairman of the Board of Directors of the Parent Company, the Chief Executive Officer and General Manager of the Parent Company (GCEO), and the Board of Statutory Auditors of the Parent Company, where the report concerns a **Corporate Body**;
- to the Board of Statutory Auditors, where the report concerns the **Chairman of the Board of Directors or any member of the Board of Directors**;
- to the Chairman of the Board of Directors of the Parent Company and the Board of Statutory Auditors, where the report concerns the **Chief Executive Officer and General Manager**;
- to the Chairman of the Board of Directors, the Chief Executive Officer and the General Manager, where the report concerns the **Board of Statutory Auditors or any of its members**.

If the report concerns situations of particular significance and gravity (regardless of the status of the reported parties indicated above), the Head of Breach Reporting System shall promptly inform the relevant Corporate Bodies of the Bank or its Subsidiaries, proposing the adoption of the most appropriate actions.

In accordance with the principle of confidentiality of the Whistleblower's identity and the information collected throughout the management of the report, **any shared report shall be anonymized** and shall contain only the information strictly necessary to understand the subject matter of the report.

The personal data collected will not be disclosed to Third Countries, defined as countries outside the territory of the European Union or European Economic Area.

4. Retention period

The provided personal data concerning the report and related documentation will be retained for as long as necessary for the processing of the report and, in any case, no longer than five years from the date of the communication of the outcome of the reporting procedure. Any further retention of personal data, or any portion thereof, may be ordered for the duration of any disciplinary or criminal proceedings, or in front of another relevant Supervisory or Judicial authority.

5. Methods of personal data processing

The IT procedure to process the report is managed by an external provider and guarantees the anonymity of the Whistleblower. This IT procedure provides for encryption of the personal data collected. Access to the information database by the external provider can only occur in case of maintenance on specific authorization and in any case without having direct access to the encrypted data. Upon completion of the report, a unique code is communicated to the Whistleblower that permits to track the report: it is the responsibility of the Whistleblower to write and keep this code.

The alleged perpetrator of the unlawful conduct is protected from negative repercussions resulting from the report, if the process does not reveal elements that justify the adoption of measures against them or, in any case, from any negative effects other than those envisaged by the specific procedure.

6. Whistleblowing process

The personal data provided as part of the Whistleblowing reporting process, using the IT platform, accessible through web link published on the corporate intranet, will be handled by the Head of the Breach Reporting System and, more specifically:

- by the Supervisory Body of BFF Bank S.p.A. in its capacity as Head of the Breach Reporting System, and by the persons authorized by it and involved in the investigative activities;
- by the Head of the Internal Audit Function of BFF Bank S.p.A. and their staff, to carry out the initial analysis phases of the reports, in relation to their independent hierarchical position;
- by the Manager of the Compliance & AML Function of BFF Bank S.p.A., if the report concerns one of the members of the Supervisory Board (in order to manage conflicts of interest) or, in the event of prolonged absence (exceeding two weeks) of the Head of the Breach Reporting System.

Personal data will be processed by the authorized persons, by computer and manual methods, according to logical criteria compatible and functional with the purposes for which the personal data were collected, to ensure the confidentiality of the Whistleblower's identity and the content of the report and related

documentation, adopting appropriate technical and organizational measures to protect them from unauthorized or illegal access, destruction, loss of integrity and confidentiality, even if accidental.

To guarantee the confidentiality of the Whistleblower for the entire duration of the processing of the report, the Whistleblower's identity will be known only by the authorized persons. Unless liability on the grounds of slander and defamation can be established or its knowledge is essential for the defense of the reported person, the Whistleblower's identity is protected in all circumstances following the report. Therefore, except for the aforementioned exceptions, the Whistleblower's identity may not be disclosed without their express consent, and all those who receive or are involved in the processing of the report are required to protect the confidentiality of that information.

7. Provision of data

The provision of personal data is optional. Howevere, non-provision of such personal data could compromise the preliminary investigation on the report: anonymous reports will be evaluated only if they are specific, detailed, and supported by appropriate documentation, enough to reveal events and circumstances connected to specific situations.

In the case of reports made anonymously, depending on the information provided, it may still be possible to deduce the identity of the Whistleblower. In any case, the Joint Data Controllers undertake to respect the Whistleblower's anonymity and not to communicate information regarding their identity. If the Whistleblower wishes to remain anonymous, they should be careful not to provide any personal information (e.g., their name or what relationship they have to the reported person) or other information that would provide information regarding their identity.

8. Rights of data subjects

The data subject has the right to obtain from the Joint Data Controllers, when applicable, access to, rectification or erasure of their personal data, or the restriction or objection to their processing (Art. 15 et seq. of the GDPR). The request may be submitted to the Joint Data Controllers through the proper channels or, alternatively, to the DPO at the e-mail address indicated above.

The exercise of the aforementioned rights could be delayed, limited or excluded with a motivated communication promptly delivered to the data subject, unless it would likely compromise the purpose of said limitation, for the period of time and within the limits in which this would represent a necessary and proportionate measure, considering the fundamental rights and legitimate interests of the data subject. In such cases, the data subject is entitled to exercise the aforementioned rights through the Supervisory Authority for the Protection of Personal Data.

9. Right to lodge a complaint

Whenever the data subject considers that the processing of their personal data is performed in violation of the provisions of the GDPR, they have the right to lodge a complaint, as provided for in Article 77 GDPR, or the right for an effective judicial remedy (Article 79 GDPR).