PRIVACY NOTICE
WHISTLEBLOWING SYSTEM

INTRODUCTION

The protection of personal data is important to the BNP Paribas Group, of which IFITALIA S.p.A. is a part. To this end, the Group has adopted strict principles and specific rules in its own *Group Personal Data Privacy Charter*, which can be consulted at the www.ifitalia.it website.

This Privacy Notice ("**Notice**") provides clear and detailed information on how we process Your personal data in the event that we receive a report from You through the BNP Paribas Group's "Whistleblowing System". The purpose of this Privacy Notice therefore is to inform You about: (i) what personal data we collect and process about You; (ii) the reasons and purposes for which we process Your personal data; (iii) with whom we share Your personal data; (iv) how long we keep Your personal data; (v) what Your rights are (regarding the control and management of your personal data) and how You can exercise those rights.

Please note that the Whistleblowing System is the instrument that enables employees of the BNP Paribas Group and certain external Third Parties connected in various ways to the Group (for example, self-employed workers, suppliers of goods and services, consultants, freelancers, trainees, volunteers, job applicants, former employees, shareholders, persons with administrative, control, supervisory or representative functions, etc.) to report acts and/or facts that may constitute a breach, even if only potential, of the Group's internal and/or external regulatory provisions (including any breaches of the BNP Paribas Group Code of Conduct).

More specifically, it is possible, through the Whistleblowing System, to report on the following issues:

A) "Professional Ethics", "Graft and Corruption", "Market Integrity", "Customers' Interests", "Protection of the Group", "Involvement with the Company and Don't Know";

B) "Respect for People";

C) "Money Laundering and Financing of Terrorism" and "Financial Sanctions and Embargoes".

The use of this System entails, depending on the subject being reported, a specific processing of data.

You will consequently find the details of the related privacy notices below.

A) WHISTLEBLOWING - OTHER ISSUES *("Professional Ethics", "Graft and Corruption", "Market Integrity", "Customers' Interests", "Protection of the Group", "Involvement with the Company" and "Don't Know")*

1. Identity of the Data Controller

Your personal data will be processed by International Factors Italia S.p.A. ("**IFITALIA**" or the "**Company**"), in its capacity as Data Controller, the details of which are set out below:

International Factors Italia S.p.A., with its registered office at Via del Mulino 9, 20057 Assago (MI), a company subject to the management and coordination of BNP Paribas S.A. - Paris (BNP Paribas Group). Website: www.ifitalia.it.

2. What personal data about You do we collect and process?

The reporting processes include the possibility that the following personal data referring to You may be processed:

- identification data (e.g. first name, surname);
- contact data (e.g. mobile phone, e-mail, postal address);
- data relating to Your occupation (e.g. employee/seconded/external collaborator, company to which You belong);
- any further information You indicated in Your report in order to substantiate the circumstances of the incident;
- any data collected in the course of any investigations that were carried out as a result of Your report.

In the event that for the purposes of Your report, You deem it necessary to provide us with special data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, data concerning health or sexual life or sexual orientation), we will only process such data if it is exclusively necessary for the examination of Your report (otherwise it will be immediately deleted) and for the sole purpose of managing the said report.

These are possible circumstances that cannot be foreseen by the Data Controller as they are left to Your judgement. In these cases, however, the processing of the data in question will be only that which is strictly necessary to follow up the report in the context of which such data was provided and always and exclusively to fulfil the legal obligation as set out in greater detail in the paragraph below

3. Why and on what legal basis do we process Your data?

We process Your personal data in order to better investigate the acts and/or facts reported by You and of which You have become aware in the context of Your employment (as an employee) or in Your capacity as a Third Party, i.e. as a person connected in various ways to IFITALIA (such as, for example: a self-employed worker, supplier of goods and services, subcontractor, consultant, freelancer, trainee, volunteer, job applicant, former employee, shareholder, person with administrative, control, supervisory or representative functions, etc.), in as much as such acts and/or facts may constitute a violation of national and/or European Union law provisions that affect the public interest or the integrity of IFITALIA, as well as unlawful conduct which may also constitute a violation of the provisions of the Organisation and Control Model adopted by IFITALIA pursuant to Legislative Decree no. 231 of 8 June 2001, as amended and supplemented.

The legal basis for the processing of Your personal data, as listed in the specific paragraph, is represented by the need to comply with a legal obligation. More specifically, the processing is necessary and indispensable in order to implement the regulatory provisions set out in Legislative Decree No. 24 of 10 March 2023 governing "*the protection of those who report violations of European Union law and laying down provisions concerning the*

protection of those who report violations of national laws".

4. How do we process Your personal data, with what means and how long do we store them?

Your personal data will be processed in accordance with the principles of relevance and non-excess in relation to the purpose pursued and of the minimisation of data processing, taking care to ensure appropriate safeguards to avoid any kind of disclosure of information.

The reports may be submitted:

1) in writing, by ordinary mail or by computerised means through the *tool* called the "Whistleblowing Platform"; or

2) orally, by means of telephone lines or, at the request of the person making the report, by means of a face-to-face meeting set within a reasonable period of time, subject to the necessary safeguards (in particular, among others, the consent of the person concerned where requested).

The processing shall be carried out by means of computerised, telematic and/or manual instruments, for the period strictly necessary for the pursuit of the aforementioned purposes and, in any case, no longer than 5 (five) years from the date of the communication of the final outcome of the reporting procedure.

5. With whom do we disclose Your personal data?

Your personal data will be processed, guaranteeing maximum confidentiality and on the basis of the *need to know* principle, only by staff belonging to the IFITALIA *Team*, specifically trained, which - on the basis of the internal *pro tempore* organisation in force at the time - is in charge of managing and assessing the reports to which this Policy Notice refers.

Please also note in this regard that the parent company BNP Paribas S.A. acts as the "Data Processor" for the processing of Your personal data in the context of the management of Your report.

In the event that, in order to follow up Your report, it becomes necessary to transmit all or part of the information collected to other IFITALIA persons not belonging to the aforementioned *Team* (e.g. experts/specialists for particular issues), such transmission will be confined to a limited number of persons expressly authorised and in any case bound by a written confidentiality obligation.

6. The transfer of personal data to a third Country or an international organisation outside the European Union

With respect to international transfers out of the European Economic Area (hereinafter also referred to as the "**EEA**"), Your personal data will only be disclosed if the European Commission recognises an adequate level of data protection for the recipient non-EEA Country.

For transfers to non-EEA Countries whose level of protection has not been recognised by the European Commission as adequate, we will rely on an exemption applicable to the specific situation or adopt one of the following appropriate safeguards to ensure the protection of Your personal data:

- Binding Corporate Rules (hereinafter also referred to as the "**BCR**"), which ensure the majority of data transfers (where applicable within the Group, already operational for some suppliers);
- in the event that the BCRs are not applicable, additional legislative instruments (e.g. "*Standard Contractual Clauses*" or "SCC"; specific consent) may be used.

The transfers in question will be carried out in compliance with Recommendations 1-2020 of the *European Data Protection Board.*

7. What are Your rights and how can You exercise them?

The law grants You, in compliance with the regulatory provisions set out in EU Regulation 2016/679 (the so-called *General Data Protection Regulation* or "GDPR"), the following rights[1]:

- Right of access (art. 15 of the GDPR);
- Right to rectification (art. 16 of the GDPR);
- Right to erasure (art. 17 of the GDPR);
- Right to restriction of processing (art. 18 of the GDPR);
- Right to data portability (art. 20 of the GDPR);
- Right to object (art. 21 of the GDPR).

In the event that You wish to exercise these rights:

1) in the event that You have submitted the report in writing by computerised means through the "Whistleblowing Platform", You can directly access the Platform (via the following link: https://secure.ethicspoint.eu/domain/media/it/gui/110837/follow.html) - more specifically to the section dedicated to updates relating to the reports submitted - by using the password created by You and the report code communicated by the system when You entered and sent the report, formulating Your request in the text space dedicated to *"Questions and Comments"*, and attaching a scan of Your identity document. We advise You to carefully keep the password You have created and the reporting code generated by the system when You enter and send Your report, as their use is essential for the exercise of Your rights and, in the event of their loss, they cannot be recovered/regenerated by the system itself;

2) if You have made the notification in writing by ordinary mail, You may use the same means of ordinary mail, making Your request to: "BNL S.p.A., Ethics Alert Device, Compliance Area BNL, Viale Altiero Spinelli 30, 00157 Rome";

3) if You have made the report orally (i.e. by telephone interview or face-to-face meeting), You may request in writing an appointment at the ordinary mail address: "BNL S.p.A., Ethics Alert Device, Compliance Area BNL, Viale Altiero Spinelli 30, 00157 Rome", specifying Your wish to exercise Your rights by means of a face-to-face meeting or telephone interview.

In order to safeguard against any unlawful processing of Your personal data, we inform You that You have the right to lodge a complaint with the Italian Data Protection Authority - Garante per la protezione dei dati personali (or any other competent supervisory Authority in the Country where You work) and/or to appeal to the competent Judicial Authorities.

8. Who is the Data Protection Officer?

We wish to inform You that IFITALIA, in its capacity as Data Controller, has appointed a *Data Protection Officer* ("DPO") who may be contacted, to obtain information on matters relating to the processing of Your data, at the following addresses:

---

[1] Rights:
- the right of access, which gives You the right to obtain confirmation from the Controller as to whether or not Your personal data is being processed and, if so, to obtain access to that data;
- the right to rectification, which allows You to obtain from the Controller the rectification and/or integration of Your personal data that is inaccurate and/or incomplete;
- the right to erasure, which allows you, in specific cases, to obtain from the Controller the erasure of Your personal data;
- the right to restriction of processing, which allows You, in specific cases, to limit the processing of Your personal data by the Controller;
- the right to data portability, which allows You, in specific cases and with respect only to the data You have provided, to request to receive Your personal data in a structured, commonly used and machine-readable format;
- the right to object, which allows You to object to the processing of Your personal data under certain conditions.

- ordinary mail: Banca Nazionale del Lavoro S.p.A., Viale Altiero Spinelli, 30 - 00157 Rome - Risk Area - Data Protection Officer (DPO)
- electronic mail: italydataprotectionofficer@bnpparibas.com

9. How can You be updated about changes to this Privacy Notice?

In a world of constant technological change, we need to periodically update this Privacy Notice. We therefore invite You to consult the updated *online* version.

B) WHISTLEBLOWING – ISSUES RELATING TO HUMAN RESOURCES *("Respect for People")*

IFITALIA and the BNP Paribas Group place great importance on the development of their employees and are committed to providing them with a motivating working environment in which all people are treated with respect, dignity and fairness. The Group pays particular attention to ensuring that these issues are not ignored, by also defining strict principles set out in the "Respect for Colleagues" section of the BNP Paribas Group Code of Conduct.

In order to ensure that everyone can work in an environment of mutual respect, the BNP Paribas Group requires each employee and each person connected in various ways to the Group to report any behaviour that may fail to meet the standards of conduct on "Respect for People", in which he or she is involved as a victim or witness.

With this Privacy Notice, therefore, as "Joint Controllers" of the processing of Your personal data, IFITALIA and its Parent Company BNP Paribas S.A. wish to provide You with clear and detailed information on how we process Your personal data should we receive a report from You through the "Whistleblowing System" concerning "Respect for People" issues.

1. Identity of the Joint Data Controllers

Your personal data will be processed by International Factors Italia S.p.A. ("**IFITALIA**" or "**Company**") as well as by BNP Paribas S.A. ("**BNP Paribas**") in their capacity as "Joint Data Controllers", the details of which are set out below:

- International Factors Italia S.p.A., a company incorporated under the laws of Italy, with its registered office at Via del Mulino 9, 20057 Assago (MI), a company subject to the management and coordination of BNP Paribas S.A. - Paris (BNP Paribas Group). Website: www.ifitalia.it.
- BNP Paribas S.A., a company under French law, with its registered office at 16 rue de Hanovre, 75002 Paris, parent company of the BNP Paribas Group. Website: www.bnpparibas.it.

The relationship among the Joint Data Controllers is specifically governed by a specific written agreement in compliance with Article 26 of the GDPR (as it is *hereinafter* defined).

2. What personal data about You do we collect and process?

The reporting processes include the possibility that the following personal data referring to You may be processed:

- identification data (e.g. first name, surname);
- contact data (e.g. mobile phone, e-mail, postal address);
- data relating to Your occupation (e.g. employee/seconded/external collaborator, company to which You belong);
- any further information You indicated in Your report in order to substantiate the circumstances of the incident;
- any data collected in the course of any investigations that were carried out as a result of Your report.

In the event that for the purposes of Your report, You deem it necessary to provide us with special data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, data concerning health or sexual life or sexual orientation), we will only process such data if it is exclusively necessary for the examination of Your report (otherwise it will be immediately deleted) and for the sole purpose of managing the said report.

These are possible circumstances that cannot be foreseen by the Data Controllers as they are left to Your judgement. In these cases, however, the processing of the data in question will be only that which is strictly necessary to follow up the report in the context of which such data was provided and always and exclusively to fulfil the legal obligation as set out in greater detail in the paragraph below.

3. Why and on what legal basis do we process Your data?

We process Your personal data in order to better investigate the acts and/or facts reported by You and of which You have become aware in the context of Your employment (as an employee) or in Your capacity as a Third Party, i.e. as a person connected in various ways to the BNP Paribas Group (for example, as: a self-employed worker, supplier of goods and services, subcontractor, consultant, freelancer, trainee, volunteer, candidate for employment, former employee, shareholder, person with an administrative, control, supervisory or representative function, etc.) which may constitute a violation of the provisions of the BNP Paribas Group Code of Conduct with particular reference to the section "Respect for Colleagues".

The legal basis for such processing of Your personal data is represented **by the pursuit of the legitimate interests of the** Joint Data Controllers in particular, the interest of IFITALIA and BNP Paribas in promoting the development and well-being of their employees, preventing and mitigating any possible conduct that may be contrary to the fundamental values of respect, dignity and fairness.

In all cases, our legitimate interests remain commensurate with Your fundamental rights and freedoms.

Any particular data You provide in Your report, insofar as they are relevant to the same and strictly necessary for its examination, will be processed as manifestly made public pursuant to Article 9, paragraph no. 2 letter (e) of the GDPR (as *hereinafter* defined).

4. How do we process Your personal data, with what means and how long do we store them?

Your personal data will be processed in accordance with the principles of relevance and non-excess in relation to the purpose pursued and of the minimisation of data processing, taking care to ensure appropriate safeguards to avoid any kind of disclosure of information.

Reports may be made exclusively in writing, by computerised means, through the *tool* called the "Whistleblowing Platform".

The processing will be carried out using computerised means, for the period strictly necessary for the pursuit of the aforementioned purposes and, in any case, for no longer than 10 (ten) years from the date of communication of the final outcome of the whistleblowing procedure.

5. With whom do we disclose Your personal data?

Your personal data shall be processed, guaranteeing the maximum confidentiality and in accordance with the *need to know* principle, only by staff belonging to the IFITALIA's specifically trained staff , who - in accordance with the *pro tempore* internal organisation in force at the time - are entrusted with the management and assessment of the reports to which this Privacy Notice refers.

In the event that, in order to follow up Your report, it becomes necessary to transmit all or part of the information collected to other persons (e.g. experts/specialists for particular issues), such transmission shall be limited to a limited number of persons expressly authorised and in any case bound by a written confidentiality obligation.

For certain and very specific cases (such as, for example, if the report involves employees holding *senior management position*), IFITALIA might share Your data with the Parent Company BNP Paribas and its supplier Navex Global Inc.

6. The transfer of personal data to a third country or an international organisation outside the European Union

With respect to international transfers out of the European Economic Area (hereinafter also referred to as the "**EEA**"), Your personal data will only be disclosed if the European Commission recognises an adequate level of

data protection for the recipient non-EEA Country.

For transfers to non-EEA Countries whose level of protection has not been recognised by the European Commission as adequate, we will rely on an exemption applicable to the specific situation or adopt one of the following appropriate safeguards to ensure the protection of Your personal data:

- Binding Corporate Rules (hereinafter also referred to as the "**BCR**"), which ensure the majority of data transfers (where applicable within the Group, already operational for some suppliers);
- in the event that the BCRs are not applicable, additional legislative instruments (e.g. "*Standard Contractual Clauses*" or "SCC"; specific consent) may be used.

The transfers in question will be carried out in compliance with Recommendations 1-2020 of the *European Data Protection Board.*

7. What are Your rights and how can You exercise them?

The law grants You, in compliance with the regulatory provisions set out in EU Regulation 2016/679 (the so-called *General Data Protection Regulation* or "GDPR"), the following rights[2]:

- Right of access (art. 15 of the GDPR);
- Right to rectification (art. 16 of the GDPR);
- Right to erasure (art. 17 of the GDPR);
- Right to restriction of processing (art. 18 of the GDPR);
- Right to data portability (art. 20 of the GDPR);
- Right to object (art. 21 of the GDPR).

Should You wish to exercise these rights, You may directly access the "Whistleblowing Platform" (via the following link: https://secure.ethicspoint.eu/domain/media/it/gui/110837/follow.html) – and more specifically in the section dedicated to updates relating to the reports submitted - by using the password You created and the report code communicated by the system when You entered and sent the report, by formulating Your request in the text space dedicated to *"Questions and Comments"*, and attaching a scan of Your identity document. We advise You to carefully keep the password created by You as well as the reporting code generated by the system when You enter and send Your report, as their use is essential for the exercise of Your rights and, in the event of their loss, they cannot be recovered/regenerated by the system itself.

In order to safeguard against any unlawful processing of Your personal data, we hereby inform You that You have the right to lodge a complaint with the Italian Data Protection Authority - Garante per la protezione dei dati personali (or any other competent supervisory Authority in the Country where You work) and/or to appeal to the competent Judicial Authorities.

8. Who is the Data Protection Officer?

We inform You that the Joint Data Controllers have each appointed a *Data Protection Officer* ("DPO") who can

[2] Rights:
- the right of access, which gives You the right to obtain confirmation from the Controller as to whether or not Your personal data is being processed and, if so, to obtain access to that data;
- the right to rectification, which allows You to obtain from the Controller the rectification and/or integration of Your personal data that is inaccurate and/or incomplete;
- the right to erasure, which allows You, in specific cases, to obtain from the Controller the erasure of Your personal data;
- the right to restriction of processing, which allows You, in specific cases, to limit the processing of Your personal data by the Controller;
- the right to data portability, which allows You, in specific cases and with respect only to the data You have provided, to request to receive Your personal data in a structured, commonly used and machine-readable format;
- the right to object, which allows You to object to the processing of Your personal data under certain conditions.

be contacted, to obtain information on matters relating to the processing of Your data, at the following addresses:

- for IFITALIA
  - ordinary mail: Banca Nazionale del Lavoro S.p.A., Viale Altiero Spinelli, 30, 00157 Rome, Risk Area, Data Protection Officer (DPO)
  - electronic mail: italydataprotectionofficer@bnpparibas.com
- for BNP Paribas
  - ordinary mail: BNP Paribas SA, Permanent Control - Fair Management - Group Communications - ACI code CAT06A1 - 16 rue de Hanovre -75002 Paris, France
  - website: www.bnpparibas.it

9. How can You be updated about changes to this Privacy Notice?

In a world of constant technological change, we need to periodically update this Privacy Notice. We therefore invite You to consult the updated *online* version.

C) WHISTLEBLOWING – OTHER ISSUES *("Money Laundering and Terrorist Financing" and "Financial Sanctions and Embargoes")*

IFITALIA and the BNP Paribas Group, as entities operating in the banking and financial sector, are subject to stringent anti-money laundering and anti-terrorist financing obligations. In this regard, the Group possesses a solid system, both at a central level and at the level of individual entities, for preventing and combating money laundering and the financing of terrorism, as well as a mechanism for complying with "International Sanctions" (i.e. all economic or trade sanctions including laws, regulations, restrictive measures, embargoes, asset freezes, that are imposed, regulated, administered or implemented by the Italian Republic, the European Union, the US Treasury Department, the Office of Foreign Resources Control, and any other competent authority).

In order to ensure the full implementation of its own provisions, the BNP Paribas Group requests each employee and every person connected in any way to the Group to strictly comply with all the obligations laid down in relation to the fight against money laundering and terrorist financing and in relation to "International Sanctions", by reporting any act and/or fact that may constitute a violation of the aforementioned obligations, of which he/she has become aware.

Consequently, by means of this Privacy Notice, IFITALIA and its parent company BNP Paribas S.A. as "Joint Data Controllers" of Your personal data, wish to provide You with clear and detailed information on how we process Your personal data in the event that we receive a report from You through the "Whistleblowing System" concerning "Money Laundering and Terrorist Financing" and "Financial Sanctions and Embargoes".

1. Identity of the Joint Data Controllers

Your personal data will be processed by International Factors Italia S.p.A. ("**IFITALIA**" or "**Company**") as well as by BNP Paribas S.A. ("**BNP Paribas**") in their capacity as "Joint Data Controllers", the details of which are set out below:

- International Factors Italia S.p.A., a company incorporated under the laws of Italy, with its registered office at Via del Mulino 9, 20057 Assago (MI), a company subject to the management and coordination of BNP Paribas S.A. - Paris (BNP Paribas Group). Website: www.ifitalia.it.
- BNP Paribas S.A., a company under French law, with its registered office at 16 rue de Hanovre, 75002 Paris, parent company of the BNP Paribas Group. Website: www.bnpparibas.it.

The relationship among the Joint Data Controllers is specifically governed by a specific written agreement in compliance with Article 26 of the GDPR (as it is *hereinafter* defined).

2. What personal data about You do we collect and process?

The reporting processes include the possibility that the following personal data referring to You may be processed:

- identification data (e.g. first name, surname);
- contact data (e.g. mobile phone, e-mail, postal address);
- data relating to Your occupation (e.g. employee/seconded/external collaborator, company to which You belong);
- any further information You indicated in Your report in order to substantiate the circumstances of the incident;
- any possible data collected in the course of investigations carried out as a result of Your report (e.g. transaction data, economic, financial and tax information).

3. Why and on what legal basis do we process Your data?

We process Your personal data in order to better investigate the acts and/or facts reported by You and of which You have become aware in the context of Your employment (as an employee) or in Your capacity as a Third Party, i.e. as a person connected in various ways to the BNP Paribas Group (for example, as: a self-employed worker, supplier of goods and services, subcontractor, consultant, freelancer, trainee, volunteer, candidate for employment, former employee, shareholder, person with an administrative, control, supervisory or representative function, etc.) that may constitute a violation of the provisions on combating money laundering and terrorist financing and/or on "International Sanctions", as well as unlawful conduct that may also constitute a violation of the provisions of the Organisation and Control Model adopted by IFITALIA pursuant to Legislative Decree no. 231 of 8 June 2001, as amended and supplemented.

The processing is necessary to ensure compliance with money laundering, terrorist financing, financial sanctions and embargoes, including at international level, for which BNP Paribas S.A. has developed a centralised system involving the various entities of the Group.

4. How do we process Your personal data, with what means and how long do we store them?

Your personal data will be processed in accordance with the principles of relevance and non-excess in relation to the purpose pursued and of the minimisation of data processing, taking care to ensure appropriate safeguards to avoid any kind of disclosure of information.

The reports concerning issues of *"Financial Sanctions and Embargoes"* may be exclusively made in writing, by computerized means, through the tool called "Whistleblowing Platform".

The processing will be carried out using computerised means, for the period strictly necessary for the pursuit of the aforementioned purposes and, in any case, no longer than 10 (ten) years and 6 months from the date of communication of the final outcome of the reporting procedure.

Reports pertaining to the issues of *"Money Laundering and the Financing of Terrorism"* may be made:

3) in writing, by ordinary mail or by computerised means through the *tool* called the "Whistleblowing Platform"; or

4) orally, by means of telephone lines or, at the request of the person making the report, by means of a face-to-face meeting set within a reasonable period of time, subject to the necessary safeguards (in particular, among others, the consent of the person concerned where requested).

The processing shall be carried outby means of computerised, telematic and/or manual instruments, for the period strictly necessary for the pursuit of the aforementioned purposes and, in any case, no longer than 10 (five) years from the date of the communication of the final outcome of the reporting procedure.

5. With whom do we disclose Your personal data?

For reports concerning the issues of *"Money laundering and terrorist financing"*, Your data will be processed, while guaranteeing the utmost confidentiality and on a *need to know* basis, only by specifically trained IFITALIA staff who - in accordance with the internal organization in force *at the time* – are in charge of managing and accessing the reports to which this Privacy Notice refers. For certain and specific cases (such as, for example, if the report requires the involvement of experts/specialists for particular issues) IFITALIA may share Your data with the Parent Company BNP Paribas in their capacity as Joint Data Controller. In any case, should it become necessary to transmit all or part of the information collected to other persons in order to follow up Your report, such transmission shall be limited to a limited number of persons expressly authorised and in any case bound by a written confidentiality obligation.

For reports concerning issues related to *"Financial Penalties and Embargoes",* Your personal data will be automatically routed to the dedicated Group channel (managed by the BNP Paribas Parent Company) and processed - while guaranteeing the utmost confidentiality and on a *need to know* basis – only by specifically trained BNP Paribas staff, who - in accordance with the internal organisation in force *at the time* – are in charge

of managing and assessing the reports to which this Privacy Notice refers.

6. The transfer of personal data to a third country or an international organisation outside the European Union

With respect to international transfers out of the European Economic Area (hereinafter also referred to as the "**EEA**", Your personal data will only be disclosed if the European Commission recognises an adequate level of data protection for the recipient non-EEA Country.

For transfers to non-EEA Countries whose level of protection has not been recognised by the European Commission as adequate, we will rely on an exemption applicable to the specific situation or adopt one of the following appropriate safeguards to ensure the protection of Your personal data:

- Binding Corporate Rules (hereinafter also referred to as the "**BCR**"), which ensure the majority of data transfers (where applicable within the Group, already operational for some suppliers);
- in the event that the BCRs are not applicable, additional legislative instruments (e.g. "*Standard Contractual Clauses*" or "SCC"; specific consent) may be used.

The transfers in question will be carried out in compliance with Recommendations 1-2020 of the *European Data Protection Board.*

7. What are Your rights and how can You exercise them?

The law grants You, in compliance with the regulatory provisions set out in EU Regulation 2016/679 (the so-called *General Data Protection Regulation* or "GDPR"), the following rights[3]:

- Right of access (art. 15 of the GDPR);
- Right to rectification (art. 16 of the GDPR);
- Right to erasure (art. 17 of the GDPR);
- Right to restriction of processing (art. 18 of the GDPR);
- Right to data portability (art. 20 of the GDPR);
- Right to object (art. 21 of the GDPR).

Should You wish to exercise these rights, for reports relating to issues of *"Financial Penalties and Embargoes"*, You may do so by accessing the Whistleblowing Platform directly (via the following link: https://secure.ethicspoint.eu/domain/media/it/gui/110837/follow.html) - and more specifically, in the section dedicated to updates on the reports You have submitted - using the password created by You and the reporting code communicated by the system when You entered and sent the report, by formulating Your request in the text space dedicated to "Questions and Comments", and attaching a scan of Your identity document. We advise You to carefully keep the password You have created and the reporting code generated by the system when You enter and send Your report, as their use is essential for the exercise of Your rights and, in the event of their loss, they cannot be recovered/regenerated by the system itself.

---

[3] Rights:
- the right of access, which gives You the right to obtain confirmation from the Controller as to whether or not Your personal data is being processed and, if so, to obtain access to that data;
- the right to rectification, which allows You to obtain from the Controller the rectification and/or integration of Your personal data that is inaccurate and/or incomplete;
- the right to erasure, which allows You, in specific cases, to obtain from the Controller the erasure of Your personal data;
- the right to restriction of processing, which allows You, in specific cases, to limit the processing of Your personal data by the Controller;
- the right to data portability, which allows You, in specific cases and with respect only to the data You have provided, to request to receive Your personal data in a structured, commonly used and machine-readable format;
- the right to object, which allows You to object to the processing of Your personal data under certain conditions.

For reports concerning the issues of: *"Money Laundering and Terrorist Financing",* instead, should You wish to exercise Your rights:

1) in the event that You have submitted the report in writing by computerised means, through the "Whistleblowing Platform", You can directly access the same Platform (though the following link: https://secure.ethicspoint.eu/domain/media/it/gui/110837/follow.html) – more specifically to the section dedicated to updates relating to the reports submitted - by using the password You created and the report code communicated by the system when You entered and sent the report, formulating Your request in the text space dedicated to *"Questions and Comments"*, and attaching a scan of Your identity document. We advise You to carefully keep the password You have created and the reporting code generated by the system when You enter and send Your report, as their use is essential for the exercise of Your rights and, in the event of their loss, they cannot be recovered/regenerated by the system itself;

2) if You have made the notification in writing by ordinary mail, You may use the same means of ordinary mail, making Your request to: "BNL S.p.A., Ethics Alert Device, Compliance Area BNL, Viale Altiero Spinelli 30, 00157 Rome";

3) if You have made the report orally (i.e. by telephone interview or face-to-face meeting), You may request in writing an appointment at the ordinary mail address: "BNL S.p.A., Ethics Alert Device, Compliance Area BNL, Viale Altiero Spinelli 30, 00157 Rome", specifying Your wish to exercise your rights by means of a face-to-face meeting or telephone interview.

In order to safeguard against any unlawful processing of Your personal data, we inform You that you have the right to lodge a complaint with the Italian Data Protection Authority - Garante per la protezione dei dati personali (or any other competent supervisory Authority in the country where you work) and/or to appeal to the competent Judicial Authorities.

8. Who is the Data Protection Officer?

We inform You that the Joint Data Controllers have each appointed a *Data Protection Officer* ("DPO") who can be contacted, to obtain information on matters relating to the processing of Your data, at the following addresses:

- for IFITALIA
  - ordinary mail: Banca Nazionale del Lavoro S.p.A., Viale Altiero Spinelli, 30, 00157 Rome, Risk Area, Data Protection Officer (DPO)
  - electronic mail: italydataprotectionofficer@bnpparibas.com
- for BNP Paribas
  - ordinary mail : BNP Paribas SA, Permanent Control - Fair Management - Group Communications - ACI code CAT06A1 - 16 rue de Hanovre -75002 Paris, France
  - website : www.bnpparibas.it

9. How can You be updated about changes to this Privacy Notice?

In a world of constant technological change, we need to periodically update this Privacy Notice. We therefore invite You to consult the updated *online* version.