GROUP WHISTLEBLOWING PROCEDURE

Issuer	Compliance
Issuer (Domain / Transversal team / OP / Region)	PE - Professional Ethics
Issuer team	PE - Professional Ethics

Functional domain	Compliance - Regulatory Compliance		
Involved Processes			
Risk domain(s)	Professional ethics (whistle-blowing)	Financial security (anti-bribery and corruption)	Financial security (embargoes & international financial sanctions)
Key procedure	Yes		
Keywords	Whistleblowing ; Alert ; Report		

Level	2
Procedure type	Procedure
Scope	Group[1]
Access rules	Public access
Owner/Author name(s)	Béatrice de Dreuille
Sponsor name(s)	Karine Mistral – de Labarthe
Validated by	Compliance EXCO

Reference	CG0038EN	
Version	VF – May 30 2018	
Status	Validated	
Date of previous version	15/09/2014	☐ N/A
Validation date	30/05/2018	
Next review date	29/05/2020	
Effective date	01/07/2018 (implementation date: 31/12/2018 – see provision on page 3)	

Higher level procedures	DG0038EN – BNP Paribas Group Code of Conduct DG0018EN – Compliance Function Charter DG0020EN – BNP Paribas Internal Control Charter
Related procedures	RHG0060EN – Procedure for managing the rights to access, correct and challenge data and handling complaints regarding Employees' personal data CG0183EN – Global Anti-corruption Policy
Regulatory texts	• French law n° 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernization of the economy of 2016 (known as the "Sapin II" Law) • French law n° 2017-399 of 27 March 2017 on duty of vigilance of parent and contracting companies • French executive order n° 2017-564 of 19 April 2017 on whistleblowing management procedures • Deliberation n° 2017-191 of 22 June 2017 from the National Data Protection Authority (CNIL) on the single authorization for the automated processing of personal data gathered through a professional whistleblowing mechanism (AU-004)

[1] "**Group**": For the application of this procedure, the term "BNP Paribas" or "Group" collectively refers to BNP Paribas S.A., its subsidiaries, and the companies controlled by it, regardless of the scope of consolidation.

	• French Anti-Corruption Agency (AFA) recommendations of December 21, 2017 • Directive 2014/65/UE of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID 2) • Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (MAR) • Regulation (EU) No 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 • Regulation (EU) No 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, and repealing Directive 95/46/EC (General Data Protection Regulation – "GDPR")

WHAT IS NEW

Due to recent regulatory developments and as part of a process of continuous improvement, the Group Whistleblowing Procedure has been thoroughly reviewed.

To this end, the present procedure, last revised on 15/09/2014:

- Strengthens whistleblowers' protection
- Broadens its scope of application as regards:
  - The persons who may use it, in order to include external Employees
  - The types of violations and matters that may be reported
- Specifies the requirements specific to the "Sanctions and Embargoes" channel
- Provides for the designation of Whistleblowing Referents
- Will be supplemented by a level 3 operational procedure[2], intended for Compliance Officers, setting out the methodological framework applicable to the receipt and handling of reports, as well as the requirements relating to privacy and data protection.

In principle, this procedure is applicable to all the Entities of the Group without transposition[3]. However, it will have to be adapted locally if countries' regulations require it.

Considering the new provisions introduced in the procedure, and the local adaptations that might be required, the implementation of the procedure may be progressive, but must be completed no later than December 31st 2018. To this end the Compliance Operational Perimeters and Regions will provide the Professional Ethics Central Domain with regularly updated implementation plans.

[2] Whistleblowing operational guide.
[3] See section 2.1 "Entities covered"

TABLE OF CONTENTS

1 Introduction

1.1 Objectives of the procedure

According to the Group Code of Conduct, Employees must report any suspected or observed breach of a law, a regulation or the Code of Conduct.

To this end, an Employee can use the whistleblowing framework presented in this procedure (the "**Whistleblowing framework**").
It is a right and no Employee will be punished for not using it.The Whistleblowing framework is not intended to replace the information to the line management or to specific procedures relating to information reporting that might exist at Group and/or local level.

The Group Whistleblowing Procedure aims to expose the rules and modalities of the Whistleblowing framework, the whistleblowing channels it is made of and the protections it guarantees to a whistleblower, subject to certain conditions. This procedure is an integral part of the Global Anti-corruption Policy (CG0183EN) in accordance with French law n° 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernization of the economy of 2016 (known as the "Sapin II" Law).

1.2 Definition of whistleblowing as per this procedure

Whistleblowing is the reporting, selflessly and in good faith, of a suspected or observed:

- Crime or offence, or
- Threat, or serious harm for the general interest, or
- Obvious and serious violation of:
  - an international norm, or
  - a unilateral act of an international organization carried out on the basis of such norm, or
  - a law or regulations, or
- Breach to the Group Code of conduct, or to a Group policy or procedure or a behavior not in the spirit of the Code of conduct,

of which the whistleblower has or had personal knowledge.

Illustration

"I suspect my colleague of accepting bribes in exchange for granting loans to clients. I witnessed several exchanges of cases containing what seems to be cash and the number of credits granted by my colleague over the past months has risen inexplicably"

☑ It is a suspected breach: *"I suspect …"*

☑ The facts reported, if true, are serious: they would constitute an offence, and a serious and obvious breach to the Code of conduct and would expose the Group to serious financial, legal and reputational risks

☑ The Employee has personal knowledge of the facts and appears to be of good faith: "*I have witnessed several exchanges…"* indicates that this is not simple hearsay *and that he/she has sufficient reasons to trust the accuracy of the facts and risks that he/she is aware of.*

1.3 Responsibility for the Whistleblowing framework

1.3.1 Responsibility for the framework

The Group's Whistleblowing framework is under the responsibility of the Group's Head of Professional Ethics Central Domain, a member of the Executive Committee of the Compliance function, reporting directly to the Head of this function. The Group's Head of Professional Ethics oversees the overall operation of the whistleblowing channels.

Within the Group Whistleblowing framework, the "Sanctions and Embargoes" dedicated channel is placed under the responsibility of Group Financial Security US (GFS US).

1.3.2 Whistleblowing Referents

Each whistleblowing channel is under the responsibility of a Whistleblowing Referent in charge of collecting and handling reports (the "**WB Referent**"). It can be a person or a team. The Referent's name and contact information must be shared with all Employees of the Entity.

At the Group level, the WB Referent is the Professional Ethics Central Domain of the Compliance function. Its contact information is displayed on the Group's "Whistleblowing" Echonet page, and mentioned at all times in the information and communication material on the WB framework.

In each Entity, as defined hereunder, the name and contact information of the Whistleblowing Referent are made available to all Employees in the Entity.

The Head of GFS US and the Head of GFS Paris are Referent for the "Sanctions and Embargoes" dedicated channel.

2 Scope

2.1 Entities covered

The procedure is applicable to all companies of the Group, regardless of their business sector, including non-consolidated controlled companies.

For the sake of this procedure, "Entity" refers to Operating Divisions, Regions, Functions, Businesses, Territories, without regard to their legal form.

In principle, the procedure is applicable without transposition. However, it will have to be adapted locally if countries' regulations require it.

2.2 Who has the whistleblowing right?

Any natural person, permanent Employee or temporary staff, and any external Staff, is authorized to use the Group's Whistleblowing framework, as long as it is used in accordance with the conditions set out in this procedure.

For the sake of this procedure, permanent and temporary Employees and external staff are collectively referred to as "Employees".

2.3 What issues can be reported through whistleblowing?

The issues that can be reported through whistleblowing include, but are not limited to:

- Acts of corruption and influence peddling or any other infringement pertaining to probity
- Acts of fraud
- Inappropriate professional behavior or lack of respect for persons, diversity, and equal opportunity (e.g. inappropriate statements and acts, discrimination, harassment)

- Infringement of the rules of professional ethics (e.g. conflict of interest in private activities)
- Infringement of the rules of financial security (e.g. money laundering, terrorist financing, non-compliance with rules regarding sanctions and embargoes)
- Anti-competitive practices (e.g. abuse of dominant position)
- Breach of market integrity (e.g. market abuse)
- Infringement of the rules for the protection of interests of clients (e.g. (ex. : charging commissions without informing the client, undue or excessive arbitration in an account under delegated management)
- Unauthorized communication of confidential information, theft or leakage of data
- Violation of human rights and fundamental freedoms, damage to the health and safety of persons or to the environment noticed within activities performed by a Group's Entity or within activities carried out by a subcontractor or a supplier within the framework of an established commercial relation with the Group or one of its Entities (e.g. if a sub-contractor is suspected of using under-aged workers).

2.4 What types of breaches can be reported through whistleblowing?

The following breach, identified within the professional framework, either suspected or observed, can be reported through whistleblowing:

- A crime or an offence
- A threat or a severe harm to general interest
- A serious and gross violation of:
    - a law or regulation (e.g. a regulations issued by the supervisory authorities)
    - an international norm (Examples: OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, European Convention on Human Rights)
    - a unilateral act of an international organization carried out on the basis of such norm (examples: UN resolutions)
- A breach of the Group Code of Conduct, or of a Group policy or procedure, or a behavior not in the spirit of the Code of conduct.

Illustration

"I suspect a colleague to disclose sensitive commercial information to a competitor (anti-competitive practice) *in the pursuance of the Group's proprietary activities"*

According to countries, some facts, information or documents might be covered secrets protected by the law. For this reason, they are not admissible in the Whistleblowing framework and cannot be disclosed (for example in France: national defense secret, or medical secret, or secret on the relations between an attorney and its client).

3 Reporting through whistleblowing

When an Employee wants to use the Whistleblowing framework, he/she shall make the report using an internal Whistleblowing channel in priority.

However, they may have the possibility, depending on the country, of using external whistleblowing channels made available by the local regulators and/or the public or legal authorities.

In some countries, precise reporting rules have to be respected by the whistleblower in order to benefit the protection system. For example in France, the reporting of an alert has to comply with a three steps process. In principle, an alert has first to be raised internally (see internal channels below). This is only if the alert has not been processed in a reasonable timeframe that the whistleblower may report externally (to the legal or regulatory authorities or professional organizations). As a last resort, if not processed by the authority or organization, within a 3 months period, the reporting may be made public.

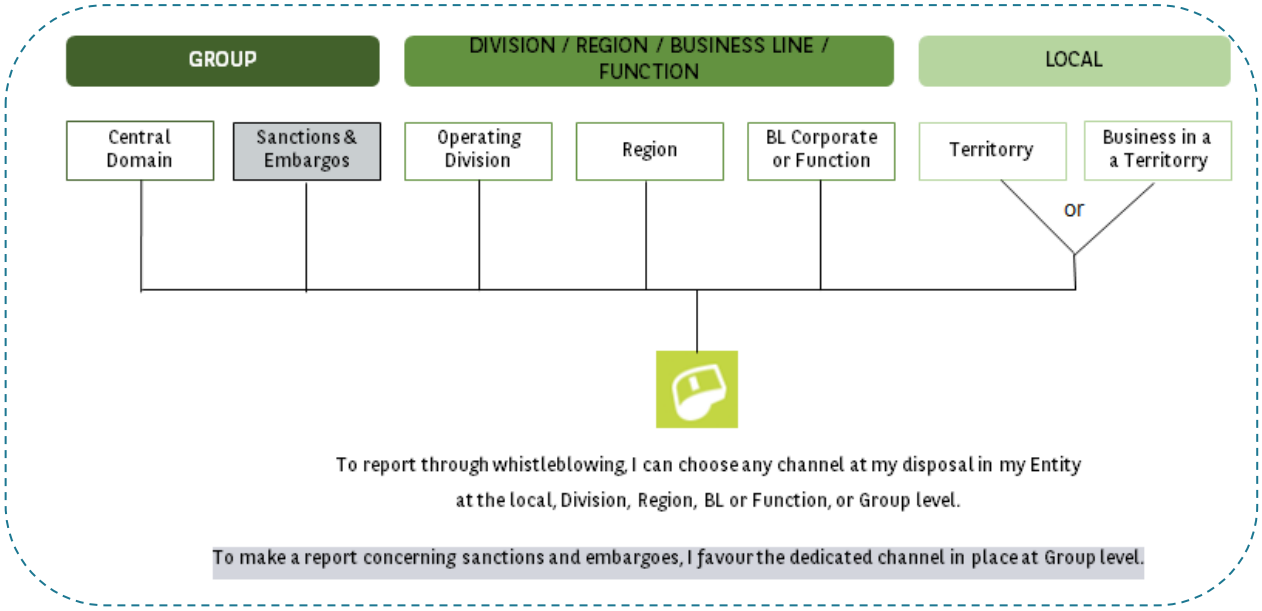
3.1 Internal channels

The Whistleblowing framework is based on the following whistleblowing channels:

1) The Group whistleblowing channel,
2) The Group "Sanctions and Embargoes" channel, dedicated to collecting reports relating to violations or other wrongdoings involving financial sanctions and embargoes.
3) A whistleblowing channel in each Operating Division (DM, CIB, IFS) and Region (Americas, APAC) and, where appropriate, at the Business Line and Function level,
4) A whistleblowing channel in each Territory level or Business in a Territory level, following the local organization of the Compliance function.

Employees have the choice of using the whistleblowing channel they want. Reports relating to sanctions and embargoes should preferably be made through the dedicated "Sanctions and Embargoes" channel, unless the local regulation provides otherwise.

Diagram of whistleblowing channels



3.1.1 Procedure for reporting in the whistleblowing channels

1) Group whistleblowing channel

Reports can be made using the following methods:

- Telephone call recorded on one of the dedicated phone lines posted on the Group "Whistleblowing" Echonet page: http://b2e.group.echonet/index.php?pid=92075
- A letter sent to the Group Whistleblowing Referent, whose address is posted on the Group "Whistleblowing Right" Echonet page
- An e-mail sent to: GLOBAL_COMPLIANCE_GROUP_ALERTE_ETHIQUE_WHISTLEBLOWING@bnpparibas.com

The report made in the Group channel must be preferably in French or in English.

2) The "Sanctions and Embargoes" channel

Reports relating to financial sanctions and embargoes can be made using the following methods, detailed in appendices:

- Submitting a report on the website managed by an external service provider located in New York: https://secure.ethicspoint.com/domain/media/en/gui/43721/index.html
- Direct telephone call to the external service provider, whose contact information is posted on the above website.

Electronic and telephone reports may be done on these platforms in the official languages of the countries in which the Group operates.

- Telephone call to one of the "Sanctions and Embargoes" Referents whose numbers are posted on the Group "Whistleblowing" Echonet page: http://b2e.group.echonet/index.php?pid=92075

The "Sanctions and Embargoes" channel is accessible in all territories, except when the laws of the country do not permit access to the above Internet and telephone platforms. In such cases, duly approved by GFS US, reports relating to financial sanctions and embargoes can be sent via the Group whistleblowing channel or the Entity whistleblowing channel.

3) The whistleblowing channel of the Entities – Territory or Business Line in a Territory, Operating Division, Region, Business Line, or Transversal Function.

Reports can be made using the methods indicated in each Entity by its Whistleblowing Referent, which may include but are not limited to:

- Telephone call to the Whistleblowing Referent, and/or
- E-mail sent to a generic address, and/or
- Filling in an electronic form available on an intranet page or a dedicated website, and/or
- Letter sent to the Whistleblowing Referent

The report can be made in any language authorized in the Entity; a report sent to an Operating Division's channel must be made in French or in English.

3.1.2 Information to be given when reporting

The whistleblower shall provide:

- All facts, information, or documents in his/her possession, regardless of their form or medium, to support his/her report[4],
- Contact information for corresponding with the Whistleblowing Referent.

3.2 External channels

When provided for by the local regulations, it is up to the Compliance function of each Entity to inform Employees about the methods for accessing the external whistleblowing channels of the local regulators and/or the public or legal authorities.

4 Handling a whistleblowing report

4.1 Steps for handling a whistleblowing report

4.1.1 Receipt

[4] See Appendices: List of information to provide when reporting through whistleblowing

The whistleblower is promptly informed (see section 4.2) by the Whistleblowing Referent of the receipt of his/her report as well as the reasonable and foreseeable time needed to carry out the initial review.

If the Employee has made an anonymous report, refer to section 5.2.

When the facts reported in the report call the Compliance function into question, the Whistleblowing Referent sends it to another Function qualified to analyze its admissibility and conduct investigations independently.

4.1.2 Initial review

The initial review consists in evaluating, at first glance, whether the report satisfies the criteria of a whistleblowing. It must not be a substitute for a further investigation.

To conduct the initial review, the Whistleblowing Referent relies on the facts and documents transmitted by the whistleblower and may contact the whistleblower as needed, if additional information is required. Other departments may be called upon, to the extent allowed by the rules relating to confidentiality as exposed in section 5.1 hereunder.

If the initial review decides that an investigation is needed, an investigation is opened. Otherwise, the procedure ends, and the whistleblower is informed of the closure of the report.

4.1.3 Investigation, decision and closure

Investigations are conducted in compliance with rules relating to confidentiality as exposed hereunder. In no case should the whistleblower try to conduct his/her own investigation.

At the end of the investigation, a formal decision is adopted (closing without further action, launching of the process of disciplinary sanction, transfer to the authorities, etc.). The adoption of this formal decision marks the closure of the whistleblowing report.

The Whistleblowing Referent informs the whistleblower and the targeted person, when required by regulations in force in the country, of the closure of the report.

The information collected in connection with the report is archived or deleted in accordance with the local regulations in force. Anonymization measures may be necessary prior to archiving, in order to protect the whistleblower's or targeted person's identity.

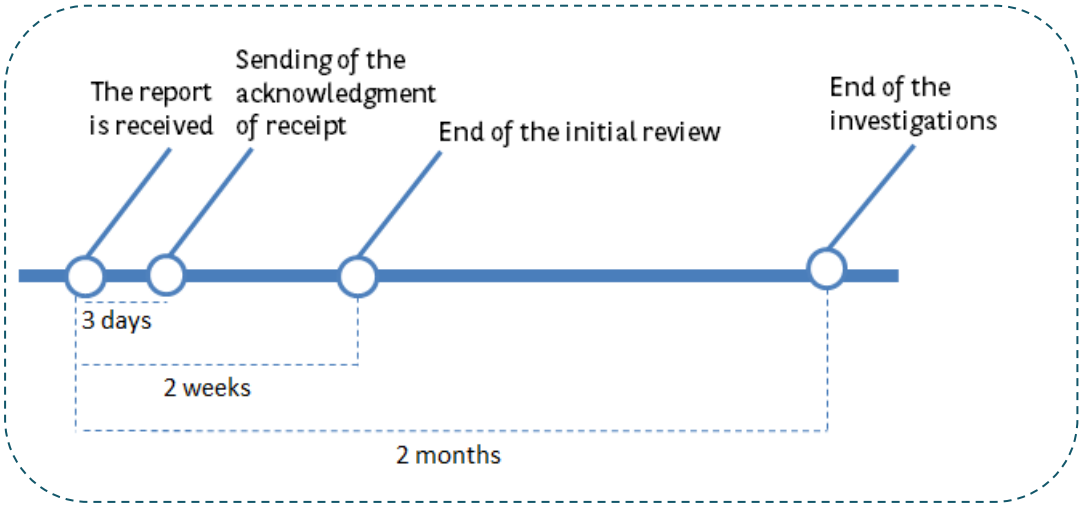
4.2 Recommended processing times

All alerts processing procedures have to include the reasonable processing times.
The following times are recommended to handle the whistleblowing report:

- A maximum of three working days, from the date the report was received, to acknowledge receipt to the whistleblower
- A maximum of two weeks, from the date the report was received, to conduct the initial review
- A maximum of two months, from the date the report was received, to finalize the investigations and inform the Whistleblower of the closure of the report.

These processing times might be adjusted depending on the circumstances and specificities of the whistleblowing.

Diagram of the steps and processing times for handling a whistleblowing report



4.3 Escalation of information

Upon receipt of a report, the Whistleblowing Referent of the Territory or Business Line or Operating Division or Region informs without delay the higher-level Referent (Operating Division or Region or Central Domain). The content and modalities of information is exposed in the Whistleblowing operational guide.

No nominative data or other information likely to reveal the identity of the whistleblower or the targeted person should be given.

5 Protections

5.1 Confidentiality

The Whistleblowing framework guarantees the confidentiality of information collected in connection with a report. Information relating to the whistleblower and the targeted person can be disclosed only if necessary, based on the “Need to know” principle, with the objective to perform the investigations and within a commitment on confidentiality.

The Whistleblowing Referent bears responsibility for compliance with the confidentiality rules. To that end, he/she takes all necessary measures, including:

- Secure storing of collected information in electronic or physical format,
- Limitation of the number of individuals informed to strictly those who need to know,
- Signing of a confidentiality charter, on a case by case basis and prior to the sending of the reports to other teams, by any person in charge of the initial review and/or investigations.

In handling a report, the Whistleblowing Referent may need to forward all or part of the information that he/she is aware of, within Compliance (for example, to experts in Financial Security, Protection of Interests of Clients, Market Integrity or to the Anti-Corruption Referent or to an Investigation Team) or to other Functions (for example, Human Resources, Inspection Générale, Legal, Risk, Communication, IT Security, CSR). Information may also need to be forwarded to the legal or regulatory authorities.

People who would have access to information pertaining to a whistleblowing are also responsible for the respect of confidentiality rules. They commit to it by signing the Confidentiality Charter which is sent to them by the Whistleblowing Referent prior to forwarding the report.

The elements enabling the whistleblower's identification cannot be disclosed without his/her consent, except to the legal authorities and to the persons in charge of handling the report who are bound to respect the above mentioned obligations of confidentiality.

Appropriate measures will be taken, in line with local laws, local regulations and the Group HR policy, against any Employee who would not respect the confidentiality rules to which he or she is committed. The disclosure of confidential information may be subject to prosecutions.

5.2 Anonymity

Unless otherwise required by local regulations, it is possible to make an anonymous report through an internal whistleblowing channel. However, when reporting, whistleblowers are strongly encouraged to communicate their identity as well as the name of the Entity in which they work.

Indeed, an anonymous report does not make it possible to acknowledge receipt of the report and to keep the whistleblower informed of the outcome of his/her report. Any anonymous report will be handled, to the extent that factual pieces of information are provided with sufficient details for establishing the seriousness of the facts and performing the investigations. It may also be more difficult or even impossible to carry out the necessary investigations if the source of the report is not identified.

5.3 Protection of the whistleblower

5.3.1 Protection against risks of discrimination and retaliation

Using the Whistleblowing framework is a right for Employees. Accordingly, no Employee may be retaliated against for an initiative that he/she takes in good faith and selflessly.

No Employee may be disciplined, discharged or discriminated against directly or indirectly with regard to recruitment, remuneration, promotion, training, assignment, or redeployment for having reported or testified to, in good faith and selflessly, a breach listed in this procedure of which he/she has or had personal knowledge.

Appropriate measures will be taken, in line with local laws, local regulations and the Group HR policy, against any Employee who would discriminate or retaliate against a whistleblower or prevent, in any way, the transmission of the report to the appropriate persons e.g. to the persons in charge of investigating).

The Compliance function shall ensure compliance with this provision in conjunction with the Group Human Resources function.

5.3.2 Other protections

Depending on the countries, additional protections might be granted by the law. For example in France: penal immunity for the person raising a report who violates some protected secrets.

5.4 Conditions to be complied with

Whistleblower protection applies only to the scope of the report. This protection cannot guard an Employee against potential sanctions for a misconduct or mistake committed previously or subsequently to the report. However, a specific protection may be granted by the regulation in some countries (for example in Italy: the whistleblower being part of the breach would benefit from a reduced criminal liability).

Any Employee who launches a report in bad faith or maliciously or with knowledge, even partial, of the inaccuracy of the alleged facts shall be liable to the penalties provided for by the rules in force. In particular, misuse of the framework may expose the reporting party to disciplinary sanctions as well as prosecution.

5.5 Protection of the person targeted by the report

The person targeted by the report is afforded the presumption of innocence.

No Employee may be disciplined, discharged or discriminated against directly or indirectly on the sole basis of the report, until further investigation concludes to his or her implication in the breach.

5.6 Data protection

To the extent that collected personal data undergoes data processing[5], the Whistleblowing Referent, as the person responsible for processing, takes all precautions needed to ensure the security and integrity of the collected data, both at the time of collection and processing of data and at the time of communication for investigation purposes and recordkeeping after the case is closed.

In accordance with procedure RHG0060 on rights to access, correct and challenge data and handling complaints regarding Employees' personal data, the whistleblower and the targeted persons (if any) have the right to access and correct personal data concerning them. In no case may the targeted person have access to data likely to identify the whistleblower.

6 Monitoring and controls of the framework

The Professional Ethics Central Domain performs the first-level of defense controls on the Group whistleblowing channel.

The Compliance function of each Entity is in charge of the first-level of defense controls of the Whistleblowing channel under its responsibility, in order to ascertain the following:

- Compliance of the framework with this procedure,
- Accessibility of the whistleblowing channels made available to Employees within the Entity.

GFS US performs the first-level of defense controls relating to the "Sanctions and Embargoes" platform.

The second-level controls of defense are presented in the Professional Ethics Generic Control Plan.

7 Employees information and awareness

Employees must be informed on the practical methods to access the whistleblowing channels and on the applicable rules. The modalities for such information are exposed in the operational guide.

Employees must be regularly made aware of their right to raise reports through the whistleblowing channels and under what conditions to use it

8 Training

The Whistleblowing Referents are trained on the receiving and handling of reports.

[5] Processing of personal data means any operation or set of operations in relation to personal data, whatever the mechanism used, especially the obtaining, recording, organisation, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

APPENDICES

Appendix 1: Glossary

ENTITY
For the sake of this procedure, “Entity” refers to Operating Divisions, Regions, Functions, Businesses, Territories, without regard to their legal form.

EXTERNAL OR OCCASIONAL STAFF
Any natural person who, although employed by a firm not part of the Group, collaborates with the Entity on a professional basis and has an extensive knowledge of the Entity’s operating mode, enabling, such as Group’s Employees, to know reprehensible risks or facts. Examples: interns are occasional staff; consultants, sub-contractors, temp are external staff.

GOOD FAITH
The whistleblower has to be utterly convinced that the information he/she discloses is genuine and must have sufficient reasons to believe that the facts and risks he has heard of are accurate. The report has to be made sincerely and without malice. People raising reports they know to be totally or partially inaccurate are excluded. Those people are exposed to prosecutions for libel. The same applies to people raising reports with the intention to harm, they are exposed to prosecutions for libel, and any unfair report is subject to disciplinary sanctions.

GROUP
For the application of this procedure, the term “BNP Paribas” or “Group” collectively refers to BNP Paribas S.A., its subsidiaries, and the companies controlled by it, regardless of the scope of consolidation.

GROUP EMPLOYEE
Any natural person working within the Group in France under an employment contract, on a secondment, or on a corporate mandate, or abroad in an equivalent situation with the Group.

PERSONAL DATA
Any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to them. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

PERSONAL KNOWLEDGE
In order to avoid defamatory or improper reports, the whistleblower may not report facts experienced by other people but may report facts that have been directly experienced by him/herself.

PROCESSING OF PERSONAL DATA
Any operation or set of operations in relation to personal data, whatever the mechanism used, especially the obtaining, recording, organization, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

SELFLESSLY
The whistleblower falls within an approach exclusively guided by the general interest. The report shall be motivated neither by a grievance nor by a personal animosity or a potential personal advantage, notably a financial reward.

WHISTLEBLOWER
Any natural person who reveals or reports, selflessly and in good faith, a crime or offence, an serious or gross breach of an international norm, of a unilateral act of an international organization carried out on the basis of such commitment, of the law or regulations, of the Group Code of conduct, policy or procedure, a potential or actual threat or severe harm to general interest, of which the whistleblower had personal knowledge.

The definition of a whistleblower depends on six cumulative criteria:

- The whistleblower is a natural person;
- The whistleblower was personally aware of the facts that he/she reports;
- The whistleblower acts selflessly;
- The whistleblower acts in good faith;
- The revealed facts are serious and fall within the scope of the issues likely to be reported
- The report is made using one of the internal whistleblowing channels made available in compliance with this procedure.

WHISTLEBLOWING

Whistleblowing is the reporting by a natural person, selflessly and in good faith, of a crime or offence, of an obvious and serious violation of an international norm, of a unilateral act of an international organization carried out on the basis of such norm, of the law or regulations, of the Group Code of conduct, policy or procedure, of a threat, or of serious harm for the general interest, potential or actual, of which the whistleblower had personal knowledge.

For the sake of this procedure, « Whistleblowing framework » refers to whole whistleblowing channels and related rules and modalities.

On the other hand, « Whistleblowing channel » refers to the mean dedicated in each Entity to address a whistleblowing report (eg: phone number and/or e-mail and/or postal address, etc.).

TARGETED PERSON

Any natural person who is reported through whistleblowing, alone or jointly with other people.

Appendix 2: Summary table of the elements of a whistleblowing as per the Group procedure

Originator of the report	**The originator of the report is a natural person.** **and** **The originator of the report is:** • **Employee**: Any natural person working within the Group in France under an employment contract, on a secondment, or on a corporate mandate, or abroad in an equivalent situation with the Group. **or** • **External or occasional staff**: Any natural person who, although employed by another firm, collaborates with the Entity on a professional basis and has an extensive knowledge of the Entity's operating mode, enabling, such as Group's Employees, to know reprehensible risks or facts. Examples: interns are occasional staff; consultants, sub-contractors, temps are external staff.
Topic of the report	**The report relates to one of the following topic (non-exhaustive list) :** • Acts of corruption and influence peddling or any other infringement pertaining to probity • Acts of fraud • Inappropriate professional behaviour or lack of respect for persons, diversity, and equal opportunity (e.g. inappropriate statements and acts, discrimination, harassment) • Infringement of the rules of professional ethics (e.g. conflict of interest in private activities) • Infringement of the rules of financial security (e.g. money laundering, terrorist financing, non-compliance with rules regarding sanctions and embargoes) • Anti-competitive practices (e.g. abuse of dominant position) • Breach of market integrity (e.g. market abuse) • Infringement of the rules for the protection of interests of clients • Unauthorized communication of confidential information, theft or leakage of data Violation of human rights and fundamental freedoms, damage to the health and safety of persons or to the environment noticed within activities performed by a Group's Entity or within activities carried out by a subcontractor or a supplier within the framework of an established commercial relation with the Group or one of its Entities (e.g. if a sub-contractor is suspected of using under-aged workers).
Breach reported	**The report relates to one of the following breach,** identified within the professional framework**, either suspected or observed :** • A crime or an offence • A threat or a severe harm to general interest • A breach of the Group Code of Conduct, policy or procedure or a behavior not in the spirit of the Code of conduct, • A serious and gross violation of: ○ a law or regulation

	○ an international norm ○ a unilateral act of an international organization carried out on the basis of such norm
Conditions to benefit from the whistleblower's status	**In addition to the abovementioned conditions, to benefit from the whistleblower's status and protections attached to it, the originator of the report must:** • Have personal knowledge of the facts: In order to avoid defamatory or improper reports, the whistleblower may not report facts experienced by other people but may report facts that have been directly experienced by him/herself. • Act in good faith: The whistleblower has to be utterly convinced that the information he/she discloses is genuine and must have sufficient reasons to believe that the facts and risks he has heard of are accurate. The report has to be made sincerely and without malice. People raising reports they know to be totally or partially inaccurate are excluded. Those people are exposed to prosecutions for libel. The same applies to people raising reports with the intention to harm, they are exposed to prosecutions for libel, and any unfair report is subject to disciplinary sanctions. • Act selflessly: The whistleblower falls within an approach exclusively guided by the general interest. The report shall be motivated neither by a grievance nor by a personal animosity or a potential personal advantage, notably a financial reward. **and** The report must have been made using one of the internal whistleblowing channels made available in compliance with this procedure.

Appendix 3: List of information to provide when reporting through whistleblowing

When reporting through whistleblowing, please indicate:

1. The location (country, Entity, company, department, ..) where the incident occurred
2. Whether you wish to remain anonymous
3. Your name, phone number, e-mail address and best time for communication with you, should you want the Whistleblowing Referent to know your identity
4. A description of the breach you want to report. Please provide as much details as possible
5. When the behaviour occurred/ began
6. How long you think the behaviour is going on
7. How you became aware of the behaviour
8. Your relationship with BNPP (e.g. Employee of the affected Entity or of another Entity, sub-contractor, …)
9. The assumed damage amount, the incident might have caused in EUR
10. The identity of the person(s) engaged in this behaviour
11. Whether you or anyone else reported the behaviour to whom
12. A list of any person(s) who may be aware of the behaviour or issue
13. A list of any person(s) who you believe have attempted to conceal this behaviour or issue
14. Any documents or files that support your report

Appendix 4: Access to the "Sanctions and Embargoes" channel

Reporting Channels dedicated to sanctions or embargo violations
Detailed Procedure

The reporting channels available to any Employee wishing to report a sanctions or embargo violation include:

1. Web Reporting Tool

In order to submit a suspected sanctions violation through the web, access the Sanctions Whistle-blower website by clicking the link:
https://secure.ethicspoint.com/domain/media/en/gui/43721/index.html or typing it directly into your web browser.

Once you access this link, you will be taken to the "Welcome" page. At the Welcome page, click on "Report a Concern" and you will be taken to the "Report Financial Sanctions or Embargos Concern" page. From the dropdown entitled, "To Make a Report Online", select the country in which you are located. Follow the reporting instructions until you are able to submit your report for review.

2. Direct Access Telephone Number to Navex

The direct access telephone number to Navex is accessible from the Sanctions Whistle-blower website (use the same web address as above). Once you get to the "Welcome" page, click "Report a Concern" and you will be taken to the "Report Financial Sanctions or Embargos Concern" page. From the dropdown entitled, "To Make a Report By Phone", select the country in which you are located for international dialling information. The direct access telephone number will be displayed with dialling instructions. After dialling the number, you will be connected to a Navex representative who will take your report information over the phone. ***Please note that in order to protect the identity of the person reporting an incident, telephone calls with Navex are not recorded or kept on file.***

If the phone line is not working, you may enter the report information through the web reporting tool or contact the Head of GFS US or Head of GFS Paris (see below for instructions).

3. Direct Access to the Head of GFS US or Head of GFS Paris

In the event you are unable to access the web or direct access telephone number to Navex, you may report a suspected sanctions violation to the following contact, as an alternative:

- the Head of GFS US – contact number: +1 212-841-3265- or
- the Head of GFS Paris – contact number: +33 (0) 1 55 77 64 38

If you cannot dial directly, contact your local operator to make a collect call, as all charges will be accepted.

In order to ensure your privacy, the identity will be kept confidential to the extent possible and applicable data privacy laws are firmly enforced for all reporting channels.