BRED Group

Whistleblowing Procedure

Issuer	DRCCP	Changes
Creation Date	January 2018	
Update	May 2018	Name of Chief Risk and Compliance Officer updated
Update	March 2020	Name of Chief Risk and Compliance Officer updated
Update	November 2021	Procedure updated
Update	January 2022	Allegation registration updated

BRED BANQUE POPULAIRE

CONTENTS

1. PREAMBLE 3
2. ACTIVITIES LIABLE TO BE NOTIFIED 3
2.1. Eligible activities 3
2.2. Exceptions to the whistleblowing right defined in law 4
3. DEFINITION OF WHISTLEBLOWER 4
4. ALLEGATION REGISTRATION MECHANISM 4
4.1. Issuing an allegation 4
4.2. Identification of the whistleblower 5
4.3. Required format 5
4.4. Reception of an allegation 5
5. ALLEGATION PROCESSING 6
5.1. Ethic officers 6
5.2. Classification of the facts 6
5.3. Assurances provided to the whistleblower 7
5.3.1. Guarantees of confidentiality 7
5.3.2. Criminal Protection 7
5.3.3. Labour Law Protection 7
5.4. Assurances provided to any other person concerned 8
5.5. Abusive utilisation of the whistleblowing mechanism 8
5.6. Archiving timeframe 8
5.7. Personal data retention period 8
5.8. Security measures 9

1. Preamble

This procedure defines the whistleblowing framework to be applied throughout the BRED Group, as provided for by:

- Law 2016-1691 of 9 December 2016 on transparency, the fight against corruption and economic modernisation (the "Sapin II" law) and Decree no. 2017-564 of 19 April 2017 (applicable to all Group legal entities);
- Law of 27 March 2017 on the duty of care and EU Directive 2019/1937 of the European Parliament of 23 October 2019 on the protection of persons who report violations of EU Law;
- Article 37 of the Decision of 3 November 2014 on internal control within companies in the banking, payment services and investment services sector subject to the supervision of the ACPR[1];
- All current or future piece of legislation, whether European or international, that incorporate a whistleblowing process.

The whistleblowing process is complementary to any other alert mechanisms implemented by the establishment. Every employee is already able to alert their line management about such matters. For banking institutions, the process is distinct from mandatory declaration procedures, such as suspicious transactions reports issued to TRACFIN or suspected market abuse, which are covered by specific procedures.

By its very nature, whistleblowing is an optional mechanism. Use of the whistleblowing system is not mandatory for employees, managers or external/temporary staff, unless required under country-specific regulations. Accordingly, no employee may be sanctioned for deciding not to use the system.

2. Activities liable to be notified

2.1. Eligible activities

Activities liable to be notified relate to:

- Any conduct or situation that is contrary to the BRED Group's code of conduct.
- Any serious act such as:
    - A crime or offense, including corruption or influence peddling;
    - A serious and clear breach of an international commitment duly ratified or approved by France;
    - A serious and clear breach of the law or applicable regulation (decrees, decisions, rules…);
    - A threat or serious prejudice to the public interest, of which the whistleblower has personal knowledge.
- Serious human rights abuses, in particular discrimination, infringement of equality, privacy, the right to strike, freedom of assembly and association, as well as infringement of fundamental freedoms, infringements of human health and safety (such as health risks), non-compliance with legal working conditions, etc.; and environmental risks.
- Any risk of actual or potential negative impacts associated with the Group’s activities or business relationships, with regard to human rights, fundamental freedoms, health and safety of persons, the environment, under the law on the duty of care.

The communicated information must relate to objective and materially verifiable facts able to substantiate the presumed nature of any violation. In order to be acted upon, data must be formulated in an objective and pertinent manner and be appropriate and directly related to the scope of the whistleblowing and be strictly necessary for subsequent verification.

[1] The administrative authority supervising financial institutions in France (*Autorité de contrôle prudentiel et de résolution* - “French Prudential Supervision and Resolution Authority”).

As all written material is liable to be made available to the authorities within the context of legal proceedings, the whistleblower must set out the facts with complete objectivity, with all the thoroughness and professionalism expected of an employee or external/temporary personnel, and in such a way as to avoid putting the entity at risk (and more generally any entity of the BRED Group) or the entity's managers or employees beyond their defined responsibilities.
The whistleblower must formulate their allegation such that it describes the presumed nature of the activity, yet under no circumstances must it compromise the private life of any employee or manager of the entity or Group, or that of any third party.

2.2. Exceptions to the whistleblowing right defined in law

Activities, information and documents covered by the following may not be revealed:

- National security;
- Medical confidentiality;
- Client-attorney privilege.

3. Definition of whistleblower

A whistleblower must be all of the following:

- a natural person
- who, in a disinterested manner and in good faith,
- reveals eligible activities
- of which they are personally aware.

For the purposes of this section, the term natural person shall be taken to mean:

- A member of the entity's personnel; or
- An external and temporary employee (even when the affiliated company has its own whistleblowing mechanism), including, but not limited to:
    - personnel provided by an external company;
    - agency staff;
    - student interns and co-op students;
    - consultants or self-employed service providers.

The whistleblowing mechanism is also made available to third parties linked to the BRED Group's activities and those of its subcontractors and suppliers for breaches of due diligence (duty of care).

Accordingly, excluded from the entity's whistleblowing mechanism is any allegation issued by a natural person without any collaborative link with the entity (e.g., a customer of the bank). However, this does not prejudge the pertinence of the allegation which may still be processed outside the context of this framework mechanism.

4. Allegation registration mechanism

4.1. Issuing an allegation

The allegation is notified to the Ethics Officers by filing an alert on a dedicated secure platform, accessible at the following URL:

https://www.bkms-system.com/BRED

This link is accessible at all times, from any connection (personal or company computer and telephone equipment). It is the same link for all BRED Group employees.

The allegation registration mechanism is not intended to replace other existing channels, namely direct or indirect line management, personnel representatives, etc. It is complementary to such channels. It is also optional, not mandatory.

4.2. Identification of the whistleblower

The identification of the whistleblower is recommended insofar as, on the one hand, the whistleblower can thus benefit from all the guarantees granted by the law and, on the other hand, because their identification makes it possible to deal with the reported failures or deficiencies in a most effective manner. The Sapin II law does not stipulate that the whistleblower must be identified.

A whistleblower who wishes to remain anonymous should be afforded the same protection as defined in section 5.3 if they are subsequently identified and subjected to reprisals. The allegation is admissible and should be counted under the following conditions:

- the seriousness of the facts mentioned is established and the factual elements are sufficiently detailed;
- the alert must be processed with particular precautions; the appropriateness of its dissemination as part of the whistleblowing mechanism must be evaluated by its first recipient.

A distinction must be made between the whistleblower and the alert as such. If the whistleblower wishes to remain anonymous, their alert is nonetheless admissible and should not be treated differently or classified differently.

4.3. Required format

The allegation shall include a minimum of:

- If the whistleblower does not want to remain anonymous: the identity and functions of the whistleblower;
- The identity, functions and contact details of the persons subject to the allegation;
- Elements enabling exchanges to take place with the recipient of the allegation, if necessary;
- The notified activities illustrating the nature of the allegation.

Where applicable, the above may be supplemented by other information and facts of which the whistleblower is personally aware.

4.4. Reception of an allegation

The recipient of the allegation must:

- Confirm receipt to the whistleblower without delay and in complete confidentiality;
- Confirm the eligibility of the allegation vis-à-vis the mechanism set out in this procedure.

To this end, the following must be verified:

- The facts are covered by the list in section 2.1 and are not covered by an exception under section 2.2;
- The whistleblower falls under one of the definitions set out in section 3;
- The allegation has been issued to the recipient in the required format.

If all of the prerequisites have been met, the recipient of the allegation shall advise the whistleblower of its admissibility within a maximum of 15 business days of receiving the allegation, via any means that guarantees strict confidentiality of the whistleblower's identity.

Should any of the prerequisites not be met, the whistleblower shall be informed of the non-admissibility of the allegation within the same deadline and under the same terms of confidentiality. All pertinent allegations shall be classified as such by the Ethics Officers.

5. Allegation processing

5.1. Ethics officers

Access to the tool for processing reports and to the content of the reports is reserved solely for the named Ethics Officers:

- Arnaud VIRICEL, Chief Risk and Compliance Officer
- Marie-Pierre SCIARA, Chief Compliance Officer
- Didier Lairie, Head of Investment Services Compliance

If the allegation concerns any of the aforementioned Ethics Officers, it will be assigned by the tool to:

- Aurélien PENNERAT, Head of Inspection Générale

5.2. Classification of the facts

An allegation judged to be admissible shall be processed within 3 months of receipt, although certain allegations may require an extension for exhaustive investigation.

The recipient of the allegation or persons specially designated to process allegations within the institution or, where applicable, entities of the BRED Group shall assess the seriousness of the allegation by means of an investigation, where necessary with the support of the competent departments while maintaining the confidentiality of the whistleblower's identity, unless agreed otherwise by the latter. The information gathered by all recipients of the allegation shall also be confidential. An undertaking of confidentiality must be signed by all persons participating in the processing of the allegation.

When registering the allegation, the whistleblower must be informed that the information gathered will be processed electronically in order to investigate and analyse the data, that the recipients of the data are persons specially designated for processing whistleblowing and that, in accordance with the French data protection act of 6 January 1978, they have a right to access and rectify their personal data, which may be exercised simply by directly contacting the recipient of the allegation designated in section 5.1. Lastly, the whistleblower is also informed that they may refuse to allow the processing of their personal data for legitimate reasons.

The person in contact with the whistleblower shall ensure that all transferred information relates to the declared eligible activities.

The processing of data provided to the recipients defined in section 5.1 shall take place using dedicated channels via electronic and/or non-electronic media.

Only the following categories of data may be processed:

- Identity, functions and contact details of the whistleblower;
- Identity, functions and contact details of the persons subject to the allegation;
- Identity, functions and contact details of the persons involved in the registration or processing of the allegation;
- The notified activities, including potentially: HR data, banking-related data, data relating to fraud…;
- Elements gathered during verification of the notified activities;
- Reports on verification measures;
- Actions taken in response to the allegation.

The facts to be gathered are strictly limited to the activities covered by the whistleblowing procedure. Allegations will only be acted upon if formulated in an objective manner, if directly related to the scope of the whistleblowing mechanism and which are strictly necessary for verification of the alleged activities. The notified activities shall be described in a manner that emphasises the presumed nature of the allegation.

Allegations registered, including those from subsidiaries outside the European Union, may be communicated to the management, control or supervisory bodies of the BRED Group, or of a BPCE Group entity, where applicable, provided such data is required for them to carry out their responsibilities.

The management of the entity shall remain free to decide the measures to be taken following the issuance of an allegation under the whistleblowing procedure by an employee, manager or external/temporary employee, within the context of the sanctions available to the institution under its internal regulations.

The whistleblower shall be informed of the measures taken in response to their allegation and, without prejudice to the assurances provided under this procedure, may be required to present their observations within the context of proceedings initiated in response to the allegation.

5.3. Assurances provided to the whistleblower

Under the conditions set out above, the whistleblower enjoys legal protection, which is provided as follows:

5.3.1.Guarantees of confidentiality

The system guarantees strict confidentiality of the identity of the whistleblower, of the persons targeted in the allegation and of the information collected, at all stages of the processing of the alert:

- the content of the allegation registered online is protected by a password;
- all exchanges between the whistleblower and the Ethics Officer, as well as the corresponding investigations and reports, are confidential;
- the number of people who deal with whistleblowing reports (the Ethics Officers) is limited and they are all subject to a strict obligation of confidentiality;
- where applicable, the experts assigned to the investigation are contractually bound to ensure the confidentiality of the data related to the professional alert and to delete them at the end of their investigations;
- Information that could identify the whistleblower may never be disclosed:
    - to the person(s) targeted in the allegations, even if they exercise their right of access under data protection law;
    - without the whistleblower's prior consent, except to the judicial authority.

Information which could identify the natural and/or legal person(s) targeted in an allegation may not be disclosed, except to the judicial authority, until the validity of the alert has been established.

5.3.2.Criminal Protection

Disclosing confidential information about the whistleblower and/or the natural and/or legal person(s) targeted in the allegation is punishable by two years' imprisonment and a fine of €30,000.

Any person who attempts to prevent the whistleblower from issuing an allegation is liable to a criminal sanction for obstructing the transmission of an alert.

Furthermore, no one may be held criminally liable for breaking confidentiality protected by the law, provided that all the following conditions are complied with:

- The disclosure is both necessary and proportionate for the protection of the interests in question;
- The disclosure complies with this procedure and falls within the scope of the whistleblowing mechanism;
- The author of the allegation meets the definition criteria of a whistleblower defined in Article 6 of law no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and economic modernisation (Article 122-9 of the Criminal Code).

5.3.3.Labour Law Protection

In accordance with the law, the BRED Group guarantees that no disciplinary measures or proceedings will be taken in connection with the disclosure under the above conditions.

The whistleblower is thus protected against any direct or indirect discriminatory measure, in particular with regard to remuneration or career development, or any disciplinary sanction or reprisal based on the fact that they have issued an alert, in accordance with this procedure.

5.4. Assurances provided to any other person concerned

Where the allegation directly or indirectly targets any other person, the entity undertakes to gather and process their personal data in compliance with the law, applicable regulations and the provisions of this procedure, notably the principles defined by CNIL[2].

Any such person shall be notified by the recipient of the allegation, if deemed necessary.

The identity of any person subject to an allegation shall be protected by the same confidentiality rules as those that apply to the whistleblower.

5.5. Abusive utilisation of the whistleblowing mechanism

Abusive utilisation of the whistleblowing mechanism, notably when targeting a person, may expose the perpetrator to sanctions or proceedings. In this regard it should be noted that false allegations, defined as those made in bad faith by a person who knows that the allegations are unfounded, is punishable by up to 5 years' imprisonment and a fine of €45,000 (Article 226-10 of the French Criminal Code).

5.6. Archiving timeframe

Data relating to an allegation that is considered by the recipient as not falling within the scope of the whistleblowing mechanism shall be destroyed without undue delay.

Where the allegation does not lead to disciplinary or judicial proceedings, the data relating to that allegation shall be destroyed or archived by the persons specially designated to manage whistleblowing allegations within two months of the conclusion of the verification.

Where disciplinary or legal proceedings are initiated against the person(s) targeted in the allegation or the whistleblower having issued an abusive allegation, the data relating to the allegation shall be retained by the persons specially designated to manage whistleblowing allegations until the conclusion of the said proceedings. Data subject to archiving measures shall be kept in a separate information system with restricted access for a period that does not exceed the duration of the legal proceedings.

5.7. Personal data retention period

Personal data related to an allegation that is considered by the recipient as not falling within the scope of the whistleblowing mechanism shall be destroyed without undue delay or anonymised in accordance with Opinion 05/2014 on Anonymisation Techniques of the European Data Protection Committee, and kept for a period of two years following the conclusion of the verification.

Where no action is taken on an allegation falling within the scope of the whistleblowing mechanism, the data relating to that allegation shall be destroyed or anonymised by the persons specially designated to manage whistleblowing allegations within two months of the conclusion of the verification. For the purposes of this framework, the term "action" refers to any decision taken by the entity to act on the allegation. This may include the adoption or modification of the entity's internal rules (internal regulations, code of ethics, etc.), a reorganisation of the entity's operations or services, the imposition of a sanction or the initiation of legal action.

[2] French Data Protection Authority (*Commission nationale de l'informatique et des libertés)*.

Should disciplinary and/or judicial proceedings be instigated following verification, the data related to the allegation shall be retained until the conclusion of the said proceedings, following which, and after any appeal periods, only data relating to the allegation shall be deleted. Data relating to the proceedings shall be archived for the usual retention periods.

With the exception of cases where no action is taken on the allegation, the recipient may keep the data collected in a temporary storage for the purpose of protecting the whistleblower or enabling the tracking of continuing offences. This retention period must be strictly limited to the objectives pursued, determined in advance and communicated to the persons concerned.

In accordance with the right to be forgotten, data should not be kept for more than 5 years from the conclusion of the verification of the allegation. Data may also be kept for longer periods in temporary storage provided that they are anonymised or if the recipient is legally obliged to do so (for example, to meet accounting, social or tax obligations).

5.8. Security measures

The recipient of the allegation and persons specially designated to manage whistleblowing allegations shall take all necessary precautions to maintain data security from registration through to communication and archiving. Access to data processing shall notably be protected by regularly renewed individual logins and passwords, or via any other means of authentication.

User sessions shall be registered and compliant use verified. The identity of whistleblowers and of persons subject to allegation, alongside the information gathered by all recipients of the allegation, shall be handled with confidentiality.