# Background information - Whistleblowing Procedure

## Why do we need whistleblowing procedure?

- *To comply with the 9 December 2016 Sapin 2 Law*
  Whistleblowing procedure is compulsory by law from 1st January 2018.

- *To strengthen our Ethics and Corporate Responsibility approach*
  Every employee is a stakeholder in risk prevention.

Whistleblowing is a system that employees have a right to use in addition to but not instead of the other existing regulatory means of expressing concerns, i.e. by informing line managers or personnel representatives. It is **optional** and only works when it is a matter of **individually-witnessed information that is communicated in good faith**.

BRL is responsible for the processing of the personal data used for the purposes of the professional whistleblowing procedure. The legal grounds that justify such processing are: - to fulfil regulatory corporate obligations, and to pursue the legitimate interests of the company (for instance, ensuring the safety of our staff).

## What is a whistleblower?

A whistleblower is someone who raises a concern, i.e. discloses inappropriate acts or omissions within the corporate entity, but has **no special interest at stake** when disclosing it and discloses it in **good faith**. The concern must be a significant and flagrant breach of an international commitment that has been duly ratified or approved by France, or of a unilateral act of an international organization based on this type of commitment, a breach of the law or regulations, a severe threat or prejudice to the public interest, a criminal offence, a wrongdoing or malpractice personally witnessed by the whistleblower. “

## When to blow the whistle

You can blow the whistle on anything that could lead to a serious breach of the law or regulations, malpractice, a wrongdoing or a criminal offence.
For instance, fraud, corruption, unfair competition, practices placing other people’s lives in danger (or their health and safety), discrimination or harassment, threats to the environment...

## How to use the whistleblowing system

If you have directly witnessed a situation or conduct that could be against the law, or a criminal offence or wrongdoing, you can report it to your line manager or use the in-house whistleblowing system, WhistleB to report your concern: https://report.whistleb.com/brlexterne.

Your report of concern must be supported by documentary evidence.
Whistleblowers are kept informed in an entirely confidential manner throughout the examination of their cases.

Exceptionally, the whistleblower is allowed to remain anonymous but the way in which the report of concern is processed depends on the following criteria:

- The serious nature of the facts reported must be established and sufficient details about the factual elements must be provided;
- Special precautions must be taken when processing the said report of concern, for instance prior examination by the first recipient of whether or not it is appropriate to disseminate the report in the frame of the whistleblowing system.

## How will a report of concern be handled?

If the concern is admissible, there will be an investigation. It will determine what measures are to be taken to end the situation of concern and, in compliance with all applicable rules, what is to be done about the person against whom the allegations are made.

The data related to a report of concern considered non-admissible upon receipt by the Concerns Recipient will be rendered anonymous and immediately destroyed or filed.

If the reported concern has not led to disciplinary action and/or legal proceedings, all related data are rendered anonymous then destroyed or filed, within two months of the closure of the verification operations. The whistleblower and the person against whom the allegations are made will be informed of the closing of the verification operations.

If disciplinary action and/or legal proceedings are brought against an alleged wrongdoer or against a wrongful whistleblower, the data related to the report of concern will be kept until the end of the procedure.

## Guaranteed safeguards and confidentiality for the whistleblower

Any person reporting a situation of concern in good faith is protected by law. It is illegal to act to the detriment of an employee or to make them redundant for reporting a concern in good faith.

This whistleblowing system is a warrant that the reports of concern and information submitted are kept entirely confidential. People in charge of collecting and processing professional reports of concern receive special training and are required to meet more stringent obligations of confidentiality.

While handing reports of concern, the accredited personnel will take all relevant precautions to ensure the confidentiality and security of the data, both during collection and during communication and storage.

The categories of data processed are: - the identification of the whistleblower, the identification of the person who is the subject of the concern, the identification of the people involved in collecting the report of concern, the facts reported, verification reports and the follow-up of the report of concern.

**Informing the person who is the subject of the concern**

The person who is the subject of the concern will be immediately informed about the situation and the reason for the report of concern so that they can oppose the processing of the data, unless interim measures are necessary to prevent the destruction of evidence. In this case, the person who is the subject of the concern will be informed when the interim measures have been taken.

The information will in particular state the facts of concern, the report of concern recipient departments and how the person can exercise their right to consult and rectify their data.

**Punishable by law**

A whistleblower using this procedure in good faith cannot be subject to disciplinary action, even if the reported facts prove to be inaccurate or have no repercussions. However, a whistleblower wrongfully using the procedure by issuing a report of concern in a wrongful manner, e.g. deliberately quoting false or inaccurate information and/or intending to cause harm, will be subject to disciplinary action and legal proceedings.

- **For a company or its employees**
  Failure to observe confidentiality is punishable by 2 years imprisonment and a fine of €30 000.
  Obstruction to reporting is punishable by one year of imprisonment and a fine of €15 000.
  Defamation of character of a whistleblower can increase the fine to €30 000 in civil litigation.

- **For a whistleblower**
  False accusations by a whistleblower are punishable by 5 years imprisonment and a fine of €45 000.

**Concerns Recipient**

The designated Concerns Recipient for all the companies in the BRL Group is the external firm, Grant Thornton.

*To consult the detailed whistleblowing procedure, go to:*
https://www.brl.fr/maj/phototheque/photos/pdf/2017/procedure_for_collection_of_reports.pdf

**Rights of people involved**

The Whistleblowing System Manager will ensure that anyone identified in the whistleblowing procedure has the right to consult the data concerning them and to have such data rectified or deleted if inaccurate, incomplete, equivocal or outdated.

Such rights of access to data can in no event allow the person who is the subject of a report of concern to obtain information about the identity of the whistleblower from the Concerns processing officer.

BRL warrants that any person identified in the whistleblowing system has a right to limited processing, a right to the deletion of data, a right to the transfer of data, a right of opposition, a right to withdraw consent and a right to express instructions applicable after their death as stipulated by law.

Anyone wishing to exercise their rights can do so by email to dpo@brl.fr or by ordinary postal letter to: The BRL Group Data Protection Officer, BRL, 1105 avenue Pierre Mendès France, BP 94 001, 30 001 NIMES Cedex 5, FRANCE

Any person involved is also entitled, if they so wish, to file a claim with the French national authorities in charge of information technologies and privacy, CNIL (Commission Nationale de l'Informatique et des Libertés). You will find more information at www.cnil.fr.

If you have any questions on the subject, please contact the Data Protection Officer at dpo@brl.fr or by ordinary postal letter to The BRL Group Data Protection Officer, BRL, 1105 avenue Pierre Mendès France, BP 94 001, 30 001 NIMES Cedex 5, FRANCE.