Information note on the "Whistleblower" system

Why use a whistleblower system?

- To meet law requirements relating to transparency, the fight against corruption and the modernization of economic life known as the "Sapin 2" law of December 9, 2016.
The law requires the establishment of a reporting system from January 1, 2018.

- Strengthen Ethics and Corporate Responsibility approach.
Each employee is involved in risk prevention.

- Protect employees
Enable everyone to report instructions which are contrary to legal or regulatory requirements

The alert mechanism is an **additional device** offered to employees which is not intended to replace other existing alert channels in application of the existing rules, in particular the hierarchical channel and staff representation bodies. Its use is **optional** and can only work **on the basis of information personally ascertained and communicated in "good faith".**

No sanction can be taken against a person who has not used this device when they were entitled to do so.

BRL has set up a Whistleblower system.

What is a whistleblower?

"The whistleblower is a person who reveals or reports, in a **disinterested manner** and in **good faith**, a serious and manifest violation of an international commitment duly ratified or approved by France, of a unilateral act by an international organization made on the basis of such an undertaking, of the law or regulations, or a threat or a serious prejudice to general interest, a crime or an offense, of which the person has personal knowledge. "

What type of alert to raise?

Anything that could lead to a serious violation of the law or regulations, a misdemeanor or a crime may be the subject of an alert.
These facts, for example, could be fraud, corruption, an unfair anti-competitive practice, endangering the lives of others (in terms of health or safety), discrimination or harassment, endangering the environment..

.

People concerned

Anyone can use the Whistleblower system, in particular :

- BRL's own staff

- BRL's employees, customers and external suppliers, which means people having a direct contractual link with the organization (consultants, agents, advisers, subcontractors natural people with an autoentrepreneur status, etc. .);

- The workforce (employees, partners, managers, etc.) legal persons that have a contractual link with BRL.

Data controllers, purposes and legal bases of processing

- BRL is responsible for the processing of personal data carried out for the purposes of managing the Whistleblowing system. The legal basis for this processing complies with regulatory obligations resulting from article 8.III of the law relating to transparency, the fight against corruption and the modernization of economic life known as the “Sapin 2” law of December 9, 2016.

The Whistleblowing system aims to allow staff members and external and / or occasional contributors to BRL to report facts relating to:
- a felony or misdemeanor;
- a serious and manifest violation of an international commitment duly ratified or approved by France ;
- a serious and manifest violation of a unilateral act by an international organization made on the basis of a regularly ratified international commitment;
- a serious and manifest violation of the law or regulations;
- a threat or serious harm to general interest, of which the issuer of the alert had personal knowledge.

The Whistleblowing system: instructions for use

If you are a direct witness of a situation or behavior that could lead to a serious violation of the law or regulations, a crime or an offense, you can report to your superiors or use the Whistleblowing system by submitting your alert on the WhistleB platform : https://report.whistleb.com/brlinterne

This platform is managed by Grant Thornton, an independent service provider, which collects alerts on behalf of BRL and performs an initial analysis to verify that the level of information transmitted is sufficient to judge the admissibility of the alert.

This report must be backed up by supporting documents.
The whistleblower will be kept informed confidentially throughout the alert process.

By way of exception, the sender of the alert may remain anonymous but the processing of their alert will be subject to compliance with the following criteria:
- The seriousness of the facts mentioned is established and the factual elements are sufficiently detailed;
- The processing of this alert will give rise to special precautions, such as a preliminary examination, by its first recipient,
 on the appropriateness of its dissemination within the framework of the disposition.

Details of the Whistleblowing system procedure are available at the address below:

https://www.brl.fr/phototheque/photos/pdf/english/procedure_for_collection_of_reports.pdf

Information for the whistleblower

People who issue a report via the system will receive relative information on treatment from the start of the alert collection process.

An acknowledgment of receipt will be provided to the whistleblower to enable them to benefit, if necessary, from a specific protection regime. This acknowledgment of receipt will be time-stamped. It will summarize all the information and, if applicable, the attachments sent as part of the report. To respect the anonymity of the whistleblower who requests it, the delivery of this receipt to the whistleblower will not be subject to the production of identifying information (email or postal address, etc.).

When a decision on the consequences of the alert has been taken by the controller, the author of the alert will be informed.

What follow-up is given to an alert? How long is the data relating to an alert kept?

If the alert is admissible, an investigation will be carried out. It will determine the measures to be taken to put an end to the situation and, in accordance with the applicable rules, against the perpetrator.

As soon as collected by the controller, any data relating to an alert considered as not falling within the scope of the system are destroyed or archived without delay, after anonymization.

When the alert is not followed by disciplinary or legal proceedings, the data relating to this alert is destroyed or archived, after anonymization, within two months of the closure of the verification operations. The issuer of the alert and the person affected by the alert will be informed of the completion of verification operations.

When disciplinary proceedings or legal proceedings are initiated against the person targeted by the alert or the author of an abusive alert, the data relating to the alert is kept until the end of the procedure.

The data can be kept longer, in intermediate archiving, if the controller has a legal obligation (for example, to comply with accounting, social or tax obligations).

Regulations relating to the protection of personal data do not apply, in particular as regards the retention periods, to anonymous data, that is to say data which can no longer be linked to one or more identified or identifiable natural persons. The data controller can therefore keep anonymized data without limitation.

What are the whistleblower's protection and confidentiality guarantees?

Anyone in good faith who makes a report is protected by law. No employee can be sanctioned or dismissed for having made a report in good faith.

The current alert system guarantees the confidential treatment of transmitted alerts and information. The people responsible for collecting and processing professional alerts are specially trained and bound by a reinforced obligation of confidentiality.

As part of alert processing, people empowered to process alerts will take all necessary precautions to preserve the confidentiality and security of data both during its collection and analysis, as well as with its communication or storage.

Categories of processed personal data

The categories of processed personal data will be : the identification of the alert giver, the identification of the alert target, the identification of those involved in the collection of the alert, the facts reported, the elements collected within the framework of the verification of the reported facts, the reports of the verification operations and the follow-up given to the alert.

Informing the person targeted by the alert

The person targeted by the alert will be informed of the facts and subject of the alert without delay, in particular to allow him to oppose the processing of this data, unless precautionary measures are necessary to prevent the destruction of evidence relating to the alert. In this case, the person targeted by the alert will be informed following the adoption of these measures.

The person will be informed of the alleged facts and the modalities of exercising his access and rectification rights.

What are the sanctions ?

The use in good faith of the Whistleblowing system will not expose the whistleblower to any disciplinary sanction, even if the facts are subsequently found to be inaccurate or are not followed up. On the other hand, the whistleblower who abuses the device by reporting an alert in bad faith, for example by communicating false or inaccurate information on purpose or with malicious intent, is liable to disciplinary sanctions as well as legal proceedings.

- Sanctions against the company or employees
Failure to maintain confidentiality is punishable by 2 years' imprisonment and a fine of € 30,000.
Obstruction of the transmission of a report is punishable by one year's imprisonment and a fine of € 15,000.
In the event of defamation against a whistleblower, the civil fine can be increased to € 30,000.

- Sanctions against the whistleblower
Slanderous denunciation by a whistleblower can be punished by 5 years' imprisonment and a fine of € 45,000.

Who are the recipients of the alerts?

The alert file is received by the referent appointed for BRL : the external firm Grant Thornton.

The data may, if applicable, be sent by Grant Thornton to the Managing Director of BRL as well as to the experts he may appoint, to the managers of the Human Resources Department and the Legal Department if necessary for verification and treatment needs of the alert or its consequences.

In addition to the aforementioned recipients, the data collected will only be accessible by legal authorities when required.

It is specified that, in accordance with legal or regulatory provisions which strictly regulate the communication of information, the elements likely to identify the issuer of the alert can only be disclosed, except to judicial authorities, with the consent of the whistleblower. Likewise, elements capable of identifying the person implicated in an alert cannot be disclosed, except to judicial authorities, until it has been established that the alert is well-founded.

People responsible for collecting and processing professional alerts are specially trained and subject to a reinforced obligation of confidentiality.

As part of the alert processing system, the people empowered to process alerts will take all necessary precautions to preserve confidentiality and security of data both during its collection and analysis, as well as its communication or storage.

Rights of the persons concerned

The person in charge of the alert system guarantees any person identified in the alert system the right to access data concerning themselves and to request rectification or deletion if they are inaccurate, incomplete, ambiguous or out of date.

The person who is the subject of an alert may under no circumstances, on the basis of their right of access, obtain information from the controller concerning the identity of the issuer of the alert.

BRL guarantees any person identified in the alert system the right to benefit from a right to limitation of processing, a right to erasure of data, a right to data portability, a right to object, a right to withdraw consent and a right to formulate post-mortem directives in accordance with applicable regulations.

- Permission to access

Anyone whose personal data is or has been processed in the context of a professional alert (whistleblower, alleged victims, persons targeted by the alert, witnesses and persons heard during the investigation, etc.), has a right to access in accordance with the provisions of Article 15 of the General Data Protection Regulation (GDPR).

The exercise of this right must not allow the person exercising it to have access to personal data relating to any other natural persons. In particular, the person who is the subject of an alert may not, under any circumstances, on the basis of their right of access, obtain information concerning the identity of the whistleblower from the controller.

This limitation is specific to the rules relating to the protection of personal data and does not preclude the application, where appropriate, of the rules of procedural law, fundamental freedoms (and in particular the principle of adversarial proceedings), etc.

- Right to object

In accordance with Article 21 of the GDPR, the right to object may not be exercised for processing operations necessary for compliance with legal obligations to which the controller is subject.

- Rights of rectification and deletion

The right of rectification, provided for in Article 16 of the GDPR, must be assessed with regard to the purpose of the processing.
In the case of the whistleblowing system, retroactive modification of the elements contained in the alert or collected during its investigation must not be allowed. When exercised, following acceptance, this right must not result in the impossibility of reconstituting the chronology of any changes to important elements of the investigation.

This right may therefore only be exercised to rectify factual data, the material accuracy of which may be verified by the data controller on the basis of supporting evidence, without erasing or replacing the data initially collected, even if incorrect.

The right to erasure is exercised in accordance with Article 17 of the GDPR.

The details of each of these rights are explained in the Personal Data Protection Charter which is accessible on the Intranet.

These rights may be exercised, at any time, by sending an e-mail to the Data Protection Officer of the BRL Group at dpo@brl.fr or by post to the attention of: Data Protection Officer, BRL Group, 1105 avenue Pierre Mendès France, BP 94 001, 30 001 NÎMES cedex 5.

Anyone concerned may also - if they so wish - lodge a complaint with the Commission National de L'informatique et des Libertés (CNIL). Further information is available on its website www.cnil.fr.

For any questions concerning these aspects, you can contact the Data Protection Officer by Email at dpo@brl.fr or by post to the attention of the Group Data Protection Officer
BRL, 1105 avenue Pierre Mendès France, BP 94 001, 30 001 Nîmes cedex 5.