



## **Procedure for collecting whistleblowing reports from BRL Group companies:**



**BRL**  
**BRL Exploitation**  
**BRL Ingénierie and its  
subsidiaries**  
**BRL Espaces Naturels**

## 1 – Purpose of the whistleblowing procedure

Since 2015, BRL's senior management has strengthened the compliance framework throughout the Group.

Implementing Decree No. 2017-564 of 19 April 2017 of the Sapin II Act specifies the rules applicable to companies with more than 50 employees in order to establish a procedure for collecting whistleblowing reports as of 1<sup>st</sup> January 2018.

This procedure has been applied since 1 January 2018 by the holding company BRL and its subsidiaries, namely BRLE, BRLEN and BRLI, and since 2025 by the subsidiaries of BRLI, following the completion of the corruption risk mapping of BRLI and its subsidiaries.

Law No. 2022-401 of 21 March 2022, aimed at improving the protection of whistleblowers, strengthened the common protection regime and broadened its scope. Implementing Decree No. 2022-1284 of 3 October 2022 on procedures for collecting and processing reports made by whistleblowers specifies the regulatory expectations of the procedure.

The system set up by the companies of the BRL Group (BRL, BRLE, BRLEN, BRLI and its subsidiaries) and described in this procedure is called *the "Professional Alert System"* and constitutes an additional channel for reporting alerts to the other existing reporting channels within the Group's companies.

Each company within the BRL Group has set up its own professional alert system using a single operating procedure.

It is based on an outsourced service that enables the collection of reports and the management of information relating to alerts in conditions of security and confidentiality that meet legal requirements.

The right to alert is an additional mechanism offered to employees. It is not intended to replace other existing alert channels, especially the hierarchical chain of command and employee representative bodies, in accordance with the rules in force. Nevertheless, individuals and/or departments that receive reports that may constitute an alert are invited to forward the case without delay, *via* the platform provided for this purpose, to the authorised persons to collect and process them.

Finally, employees have the discretionary the internal channel within the group companies, as described in this procedure, or contact one of the external bodies listed below:

- The Defender of Rights;
- An authority from the list set out in the aforementioned decree, reproduced in Appendix 4;
- The judicial authority;
- An authority of the European Union competent to receive reports of violations of European Union law.

The Group's Integrity Plan, issued by the Group's Managing Director on 24 May 2024, the BRL Group's Code of Ethics and the Codes of Conduct of the Group's companies integrate this procedure.

## 2 – Scope of the procedure

This procedure applies to all reports made by:

- **Shareholders, partners and holders of voting rights at General Meetings of BRL Group companies;**
- **Members of the Boards of Directors** of BRL Group companies;
- **Employees of BRL, BRL Exploitation (BRLE), BRL Ingénierie (BRLI) and its subsidiaries, BRL Espaces Naturels (BRLEN), external or occasional employees**, including those whose employment relationship has ended;
- **Candidates who have taken part in a recruitment process** for one or more companies within the Group;
- **Contractors** (e.g. suppliers, clients, consultants, freelancers) and subcontractors of one or more Group companies, members of their administrative, management or supervisory bodies, their subcontractors and their staff.

The whistleblowing system covers reports relating to:

- **A breach or situation contrary to the principles of the BRL Group's Integrity Plan, the BRL Group's Ethics Charter and the Codes of Conduct** of the Group's companies;
- **A crime or offence;**
- **A violation or attempted violation of:**
  - **An international commitment** ratified or approved by France;
  - **A unilateral act by an international organisation** based on such a commitment;
  - **European Union law;**
  - **A law or regulation;**
- **A threat or harm to the public interest.**

**Reports may concern breaches in several areas:**

- Corruption (active or passive, public or private)
- Health and safety
- Personal data protection
- Breaches of competition law
- Discrimination
- Harassment
- Fraud
- Obstruction of the right to report concerns.

This list is not exhaustive, and these areas are subject to change over time.

### 3 - Definition and status of whistleblowers

The law provides protection for whistleblowers are protected by law in terms of both civil and criminal liability and professional matters (Article 10 of Law No. 2016-1691 of 9 December 2016).

The status of whistleblower and the associated protection regime are recognised for:

- **Any natural person**;
- **Reporting facts of which they have become aware of in the course of their professional activities**: facts known indirectly may also be reported and give rise to whistleblower protection. If the facts were not discovered in a professional context, the person making the report must have become personally aware of them personally (either as a direct witness to the facts or as a victim);
- **Receiving no direct financial compensation**: this means that the person reporting cannot be remunerated for raising the alert if they wish to benefit from the protection afforded to whistleblowers;
- **Acting in good faith**: unless the information provided by the whistleblower clearly indicates otherwise, the whistleblower's good faith is presumed. It will only be necessary to verify the whistleblower's good faith in cases where reports have led to investigations and the whistleblower's allegations have not been verified.

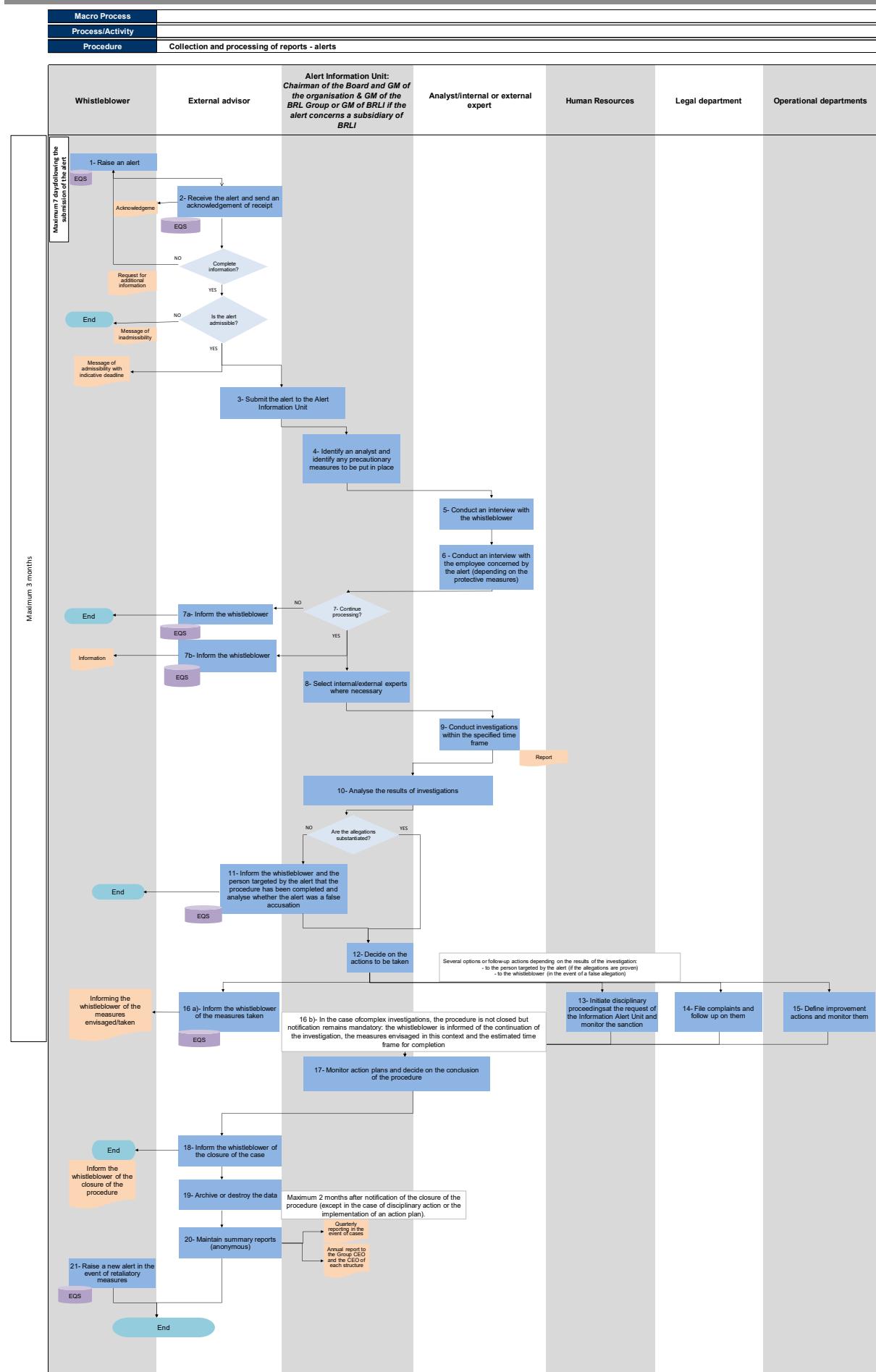
This protection can also be extended (Article 6-1 of Law No. 2016-1691 of 9 December 2016):

- **To natural and legal persons who assist the whistleblower in making a report** (referred to in the law as "facilitators"). These may be an NGO or a trade union representative, for example;
- **Natural persons connected to a whistleblower who are at risk of reprisals because of this connection** (e.g. a family member who works in the same company or in a controlled entity as the whistleblower);
- **Legal entities controlled by the whistleblower, or those for which they work or with which they have a professional connection** (e.g. a company owned by the whistleblower).

If this status is recognised, the whistleblower benefits from triple protection due to their status:

- **Criminal immunity** for the offence of breaching a legally protected secret.
- **Strict confidentiality of their identity**: their identity may only be disclosed with their consent (except to the judicial authorities).
- **Total protection of their professional situation** by the French Labour Code and the French Monetary and Financial Code against any form of discrimination following their report.

## 4 - Flowchart



## 5 - Description of the steps in the procedure

#	Steps	Documents
1	<p>Whistleblowers falling within the scope of the procedure (see 2 – <i>Scope of the procedure</i>) may submit their report <i>via</i> the EQS platform if they wish to exercise their right to report concerns (and benefit from the protection afforded to whistleblowers).</p> <p><i>Platform link: <a href="https://brl.integrityline.app">https://brl.integrityline.app</a></i></p> <p>The alert consists of:</p> <ul style="list-style-type: none"> <li>- A precise description of the observed or reported facts</li> <li>- The name and position of the person concerned by the alert</li> <li>- Supporting documents, where applicable, to back up the description</li> </ul> <p>Whistleblowers may report facts of which they have become aware of in the course of their professional activities, including those known indirectly (which may have been reported to them). They may report facts that have occurred or are very likely to occur.</p> <p>If the facts were not learned in a professional context, the person making the report must have personal knowledge of them (e.g. as a direct witness or victim of the facts).</p> <p>To benefit from the protection afforded by whistleblower status, the person making the report must be:</p> <ul style="list-style-type: none"> <li>- a natural person</li> <li>- have become aware of the information reported in the course of their professional activities<sup>1</sup></li> <li>- be acting in good faith,</li> <li>- act without direct financial compensation.</li> </ul>	<p>EQS</p> 
2	<p>The alert thus filed is received by the designated contact person for all BRL Group companies: the external firm Grant Thornton.</p> <p>As soon as the alert is received, the contact person immediately sends to the whistleblower an acknowledgement of receipt (transmitted by EQS).</p> <p>An initial analysis is carried out by the designated officer to verify that the information provided is sufficient to assess the admissibility of the report. If the information is incomplete,</p>	<p>Acknowledgement of receipt</p>

<sup>1</sup> In accordance with the amendments introduced by Law 2022-401 on 21 March 2022, whistleblowers may have indirect knowledge of the facts reported. It is now possible to report "reported" facts, provided that the whistleblower became aware of them in the course of their professional activities. Otherwise, the person making the report must have personal knowledge of the facts (either as a direct witness or victim).

	<p>the designated officer may request additional information from the whistleblower.</p> <p>The representative then analyses the admissibility of the alert based on the following criteria:</p> <ul style="list-style-type: none"> <li>- Does the alert fall within the scope of the system (see <a href="#">2- Scope of application</a>)?</li> <li>- Is the alert clear and detailed, and does it include supporting documents?</li> </ul> <p><b>There are then two possible scenarios:</b></p> <ul style="list-style-type: none"> <li>- If the alert is deemed inadmissible, the contact person informs the whistleblower of this decision and the reasons why their report is deemed inadmissible and ends the process. A message is sent to the whistleblower indicating the contacts they should reach out to if their report is deemed inadmissible, but an internal contact would be able to handle their request (e.g., a conflict between employees): The contact person then immediately destroys the data and documents relating to the alert in accordance with regulatory requirements.</li> <li>- If the alert is deemed admissible, the contact person sends a notification of admissibility to the whistleblower (within a target period of five working days following the submission of the alert, subject to any additional information that may be required), along with an indicative reasonable processing time, depending on the nature of the alert.</li> </ul> <p>All communication between the whistleblower and the contact person during this stage takes place <i>via</i> the EQS platform.</p> <p><b>An anonymous report may be considered and declared admissible under two conditions:</b></p> <ul style="list-style-type: none"> <li>- The seriousness of the facts must be clearly established;</li> <li>- The whistleblower must provide evidence that is sufficiently precise and detailed to prove the facts, beyond their testimony, which, being anonymous, could otherwise prevent it from being considered probative in subsequent proceedings.</li> </ul> <p>If the above conditions are not met, anonymous reports will be considered inadmissible.</p>	<p>Inadmissibility message</p> <p>Admissibility message with indicative deadline</p>
3	If the alert is deemed admissible, the referent is responsible for referring it to the Alert Information Unit of the company concerned by the alert. This unit is composed of the Managing Director and the Chairman of the Board of Directors of the relevant company, as well as the Managing	

	<p>Director of the parent company to which the company belongs (see Appendix 1 for a list).</p> <p>If the report made through the channel concerns events that occurred in a Group company other than the one to which the whistleblower belongs, the contact person shall take one of the following actions:</p> <ul style="list-style-type: none"> <li>- Refer the case to the Alert Information Unit of the relevant company, after informing the whistleblower.</li> </ul> <p><i>If the alert directly concerns the Managing Director of a first-tier subsidiary, it is escalated to the Chairman of the Board of Directors of that subsidiary and to the Managing Director of the BRL Group.</i></p> <p><i>If the alert directly concerns the Managing Director of the BRL parent company, it is escalated to the Chairman of the Audit and Risk Assessment Committee and the Chairman of the Board of Directors of BRL. If the alert directly concerns the Managing Director of a BRLI subsidiary, it is escalated to the Chairman of the Board of Directors of the BRLI subsidiary concerned, the Managing Director of BRLI and the Managing Director of the BRL Group.</i></p> <p>Members of the Alert Information Unit make a personal commitment by signing a letter of commitment (template in Appendix 2), in which they undertake to comply with the following obligations:</p> <ul style="list-style-type: none"> <li>- Strict confidentiality obligation;</li> <li>- Obligation of impartiality;</li> <li>- Obligation of transparency and fairness towards the persons whose data is being processed;</li> <li>- Absence of conflict of interest and obligation to declare any conflict of interest relating to a case.</li> </ul> <p>The contact person presents the constituent elements of the alert (statement of facts and mention of the persons targeted by the alert, possible facilitators, initial analysis in terms of admissibility, etc.). Only the identity of the whistleblower is not disclosed.</p> <p>The constituent elements of the alert, as well as all data relating to subsequent investigative actions, are protected by strict confidentiality and are exclusively accessible to individuals expressly authorised to receive them in accordance with this procedure.</p> <p>Disclosure of this data to any other person is strictly prohibited.</p>	
4	Based on the facts presented, the company's Information Alert Unit appoints an analyst to examine the subject matter of the alert and its capacity to conduct the initial investigations reliably and objectively (in addition to the necessary authority, skills and resources).	

	<p>The analyst also signs a letter of commitment to guarantee their independence and impartiality throughout the procedure, declaring in particular that there is no conflict of interest (see Appendix 3).</p> <p>At this stage, if necessary, the Information Alert Unit decides to implement precautionary measures in connection with the alert (file backup checks, file copies, etc.) in order to prevent the destruction of evidence by the perpetrator; among other things.</p> <p>Precautionary measures are carried out in accordance with the rules set out in the BRL Group's Information and Communication Technology (ICT) Charter.</p>	
5	<p>Once the analyst received the whistleblower's contact details from the designated contact person, they will arrange an interview with the whistleblower. During this interview, the analyst will remind the whistleblowers of the framework and procedure, their rights and obligations, and may add to or clarify certain points in the report. This initial interview should confirm the information submitted to the company's Information Alert Unit and enable the next steps in the investigation.</p> <p>In any event, the meeting with the whistleblower will be one of the following:</p> <ul style="list-style-type: none"> <li>- <b>With the whistleblower's consent</b>, it is recorded on a durable or recoverable medium accessible only to persons authorised to handle the report, in accordance with the procedure;</li> <li>- <b>Without the whistleblower's consent</b>, it is transcribed in full by the analyst in the form of minutes.</li> </ul> <p>The whistleblower then has the opportunity to check, correct and approve the minutes by signing them.</p>	
6	<p>At the same time, the employee concerned is informed and interviewed by the analyst and, where applicable, by the Human Resources Department. This interview is conducted in accordance with the principle of adversarial proceedings and the right of reply. However, if the precautionary measures decided upon also require that the employee concerned by the alert not be notified immediately, the employee will only be heard by the investigator at a later date (once the measures have been implemented, the information may be postponed until the end of the investigation measures).</p> <p>It should be noted that under no circumstances may the identity of the whistleblower, the person concerned, the</p>	

	witnesses or any person mentioned in the alert be disclosed to the employee concerned by the alert.	
7	<p>At the end of the interviews, the investigator will report to the company's Alert Information Unit and the referent.</p> <p>The company's Alert Information Unit may decide to:</p> <ul style="list-style-type: none"> <li>- Discontinue further investigations (if the interviews conducted show that the facts giving rise to the alert are not founded);</li> <li>- Continue the investigation.</li> </ul> <p>In both cases, the contact person must inform the whistleblower of the decisions taken <i>via</i> the EQS platform.</p> <p>Information regarding the investigative measures taken to assess the accuracy of the facts must be provided to the whistleblower <b>within three months of the alert being acknowledged</b>.</p> <p>In the case of complex investigations, if the duration of the investigations is extended beyond the aforementioned three-month period, this shall be done after expressly informing the whistleblower.</p>	Information
8	<p>Depending on the nature of the alert, the company's Information Alert Unit may decide to appoint experts (internal and different from the person in charge of processing or external) to carry out investigations requiring specific skills (e.g. accounting and financial skills, legal skills, etc.).</p> <p>If an external expert is used, particular vigilance is applied to the procedures for purchasing intellectual services in order to guarantee the confidentiality of the data and the identity of the parties involved.</p> <p>In addition, the analysts sign a letter of commitment to guarantee their independence and impartiality during the process, declaring in particular that there is no conflict of interest (see Appendix 3).</p>	
9	The analyst and/or selected experts (accounting and financial skills, legal skills, etc.) carry out their investigations within the specified time frame and report to the Information Alert Unit and the referent in a written report.	Investigation report
10	The company's Alert Information Unit and the analyst examine the results of the investigations and the Managing Director of the company concerned decides on the action to be taken. Two situations may then arise: <ul style="list-style-type: none"> <li>- The allegations are unfounded (step 11), and the process ends;</li> </ul>	

	<ul style="list-style-type: none"> <li>- The allegations are founded, in which case the process continues (step 12).</li> </ul>	
11	<p><i>If the allegations are unfounded:</i></p> <ul style="list-style-type: none"> <li>- The analyst must inform the person targeted by the alert of the end of the procedure, <i>via</i> an interview.</li> <li>- The referent must notify the whistleblower of the end of the procedure <i>via</i> EQS.</li> </ul> <p>The company's Information Alert Unit also decides whether or not to prosecute the whistleblower if the alert constitutes a case of slanderous denunciation, and , initiates disciplinary proceedings if necessary.</p>	Information
12	<p><i>If the allegations are founded:</i></p> <p>The company's Information Alert Unit identifies the actions to be taken and the parties responsible for taking measures to remedy the situation.</p> <p>Three different actions, presented in steps 13 to 15, may be taken. These actions may concern:</p> <ul style="list-style-type: none"> <li>- the person targeted by the alert, if they are found to be responsible for the facts (substantiated alert)</li> <li>- the whistleblower for false reporting in the event of an unfounded alert (it should be noted that no sanctions or disciplinary measures may be taken against a whistleblower who has communicated false or inaccurate information in good faith).</li> </ul> <p>If measures are taken against the person targeted for the reported acts, the whistleblower will be informed of the nature of the measures taken and the reasons for them.</p>	
13	<p>Depending on the seriousness of the facts, disciplinary proceedings may be initiated against the person targeted by the alert. These proceedings are initiated by the senior management of the company concerned and the Group's Human Resources Department, which will monitor them.</p>	
14	<p>Depending on the seriousness of the facts, legal proceedings may be initiated against the person targeted by the alert. These proceedings are initiated by the senior management of the company concerned and carried out by the Group's Legal Department, who are responsible for filing and following up on the complaint.</p> <p>In the event of false accusations, the whistleblower may also be subject to the criminal penalties provided for in Article L.226-10 of the French Criminal Code.</p>	

15	<p>In addition to disciplinary and/or legal sanctions, the company's Information Alert Unit may identify areas for improvement that must be implemented by various departments in order to ensure that malfunctions are resolved and prevented (improvement action plan or action plan related to sanctions).</p>	
16	<p>The contact person informs the whistleblower, <i>via</i> EQS, of the measures taken in the event of a founded alert (in terms of sanctions and/or action plans) and the reasons for these measures, which effectively constitutes the end of the procedure for the whistleblower.</p> <p>In all cases, the whistleblower is informed in writing of the final closure of the case once the remedial measures have been decided.</p>	
17	<p>The company's Information Alert Unit and the analyst monitor the progress of the action plans and decide on the conclusion of the investigations and the procedure at the organisational level.</p>	
18	<p>The whistleblowing officer shall systematically inform the whistleblower in writing of the final closure of the case.</p>	
19	<p>The referent must set up a system to monitor the receipt, processing and follow-up of alerts:</p> <ul style="list-style-type: none"> <li>- <u>If the alert is deemed inadmissible</u> or if the investigation does not result in disciplinary and/or legal proceedings and no action plan is adopted, the data relating to this alert must be destroyed <b>within a maximum of two months</b> from the date of notification to the author of the report being notified that the case has been closed in the system.</li> <li>- <u>If the alert leads to disciplinary and/or legal proceedings</u>, the data relating to this alert and the investigations will be <b>kept until the end of the legal proceedings or the expiry of the time limit for appealing against the decisions made</b>.</li> <li>- <u>When action plans are implemented to draw conclusions from the way the alert was handled</u>, the data is destroyed at the end of the action plan or <b>after a maximum period of six months</b> if it is necessary to monitor the absence of reprisals against the decisions rendered</li> </ul> <p>Unless <b>no action is taken on the alert</b>, the data controller may retain the collected data in the form of intermediate</p>	

	<p>archives<sup>2</sup> for the purpose of the protecting of the whistleblower or facilitating the detection of ongoing offences. <b>This retention period must be strictly limited</b> to the purposes pursued, determined in advance and brought to the attention of the persons concerned (i.e. whistleblowers, relevant individuals and witnesses) and <b>may therefore not exceed six months after the end of the litigation proceedings</b>, the expiry of the limitation period for appeals or the expiry of the action plan.</p> <p><b>The tool incorporates automatic purging systems</b> to delete data in accordance with the data controller's requirements.</p> <p><b>EQS destroys paper data using a file shredder in accordance with DIN 66399</b> or via an external service provider.</p>	
20	<p>The contact person keeps track of the status of alerts received and processed:</p> <ul style="list-style-type: none"> <li>- When cases arise, a report is sent to the Managing Director of each company prior to each Board of Directors meeting, presenting: <ul style="list-style-type: none"> <li>o an overview of ongoing cases</li> <li>o the overview of sanctions imposed</li> </ul> </li> </ul> <p>The Managing Director of each company must supplement this report with the improvement measures taken to prevent the risk and their progress.</p> <ul style="list-style-type: none"> <li>- When cases arise, a quarterly report is sent to the Managing Director of the BRL Group on the number of cases reported, admissible cases, ongoing cases, and closed cases broken down by structure and for the Group as a whole.</li> <li>- Regardless of the number of cases, an annual report on the alert system (key indicators, results of processing, average processing times, and types of cases reported), by company and for the Group as a whole, is also sent to the Managing Director of the BRL Group and to the Managing Director of each company concerning their company. An annual meeting with the representative is organised to discuss the effectiveness of the system and, if necessary, identify areas for improvement.</li> </ul>	<p>Quarterly reporting by subsidiaries where cases have been reported</p> <p>Quarterly reporting by the Group in the event of cases</p> <p>Annual report</p>
21	Within six months of the conclusion, the representative will conduct an interview to ensure that the whistleblower has not	

<sup>2</sup> In this case, the data subject to archiving measures is stored in a separate information system with restricted access and may only be consulted to ensure the protection of the whistleblower, their relatives, the legal entities they control and their employees, whistleblowing facilitators or witnesses.

	<p>been subjected to any specific measures (such as sanctions or discrimination) in connection with the alert raised.</p> <p>The results of this follow-up will be communicated to the Managing Director of each company annually.</p>	
22	<p>If the whistleblower believes they have been subjected to specific retaliatory measures (sanctions, discrimination) in connection with the alert raised, they are invited to contact the whistleblowing officers of the group companies by raising a new alert dedicated to these retaliatory measures <i>via</i> the secure platform.</p>	EQS

**Appendix 1 – List of members of the Group companies' Information Alert Units**

<b>Entity</b>	<b>Managing Director of the company</b>	<b>Chairman of the Board of Directors</b>	<b>Managing Director of the BRL Group</b>
BRL	Mr Jean-François Blanchet	Mr Fabrice Verdier	Mr Jean-François Blanchet
BRL Exploitation	Mr Franck Maruejols	Mr Fabrice Verdier	Mr Jean-François Blanchet
BRL Espaces Naturels	Mr Bruno Miara	Mr Fabrice Verdier	Mr Jean-François Blanchet
BRL Ingénierie	Mr Gilles Rocquelin	Mr Fabrice Verdier	Mr Jean-François Blanchet
<hr/>			
<b>Entity (subsidiary of BRLI)</b>	<b>Managing Director of the subsidiary</b>	<b>Chairman of the Board of Directors</b>	<b>Managing Director of BRLI (parent company)</b>
BRL Madagascar	Mr Nicolas Petitjean	Mr Gilles Rocquelin	Mr Gilles Rocquelin
BRL Ingénierie Côte d'Ivoire	Mr Vincent Auger	Mr Gilles Rocquelin	Mr Gilles Rocquelin
We Consult Uganda	Mr Julien Verdonck	Mr Gilles Rocquelin	Mr Gilles Rocquelin

## APPENDIX 2 – Letter of commitment for members of the Alert Information Unit

Dear Ms/Mr **Y**,

As part of the alert system implemented by **XXXXX**, you have appointed me to **serve as a member of the Alert Information Unit** for the following scope:

In order to guarantee the independent and impartial performance of my duties, I undertake to:

- Not having identified any potential or actual conflicts of interest in accepting this mission and to declare any such situations that may arise during the course of my duties;
- Have the necessary skills and resources to carry out this mission;
- Be familiar with the **XXXXX** company's whistleblowing procedure and undertake to comply with and implement it;
- Comply with enhanced confidentiality obligations, particularly with regard to the personal information of the whistleblower and any person mentioned in the report, throughout the investigation, under penalty of criminal sanctions<sup>3</sup>;
- Use only the tool for all exchanges with the whistleblower, for drafting interview reports and my reports, and for storing all supporting documents.

***Precede the signature of the data controller with the words "Read and approved on XX/XX/XXXX".***

---

<sup>3</sup> Disclosure of confidential information following the receipt of a report: 2 years' imprisonment and a fine of €30,000  
Page 16 of 19 – WHISTLEBLOWING PROCEDURE | V\_EN\_0725

### Appendix 3 – Letter of commitment to analysts

Dear Ms/Mr **Y**,

As part of the whistleblowing system implemented by **XXXXX**, you are authorised to **handle/investigate [choose]** the whistleblowing report referenced **[XXX]** dated **[XXX]**.

In this context, you declare:

- Not having identified any potential or actual conflicts of interest in accepting this assignment and undertaking to declare any such situations that may arise during the course of the assignment;
- I have the necessary skills and resources to carry out this assignment;
- I have read and understood **XXXXX**'s whistleblowing procedure and undertake to comply with and implement it;
- You undertake to comply with enhanced confidentiality obligations, particularly with regard to the personal information of the whistleblower and any person mentioned in the report, throughout the investigation, under penalty of criminal sanctions<sup>4</sup> ;
- You undertake to use the tool exclusively for all communication with the whistleblower, for drafting interview reports and your reports, and for storing all supporting documents.

You have **[XXX]** weeks to complete your assignment in order to ensure that the alert is processed within the legal time limits.

***Precede the signature of the data controller with the words "Read and approved on  
XX/XX/XXXX".***

---

<sup>4</sup> Disclosure of confidential information following receipt of a report: 2 years' imprisonment and a fine of €30,000  
Page 17 of 19 – WHISTLEBLOWING PROCEDURE | V\_EN\_0725

## Appendix 4 – Authorities authorised to receive reports

### **1. Public procurement:**

French Anti-Corruption Agency (AFA), for breaches of integrity;

DIRECTORATE GENERAL FOR COMPETITION, CONSUMER AFFAIRS AND FRAUD CONTROL (DGCCRF), for anti-competitive practices;

Competition Authority, for anti-competitive practices;

### **2. Financial services, products and markets, and prevention of money laundering and terrorist financing:**

Financial Markets Authority (Autorité des marchés financiers – AMF), for investment service providers and market infrastructures;

Prudential Supervision and Resolution Authority (ACPR), for credit institutions and insurance organisations;

### **3. Product safety and compliance:**

DIRECTORATE GENERAL FOR COMPETITION, CONSUMER AFFAIRS AND FRAUD CONTROL (DGCCRF);

Central Service for Arms and Explosives (SCAE);

### **4. Transport safety:**

Civil Aviation Authority (DGAC), for air transport safety;

Land Transport Accident Investigation Bureau (BEA-TT), for land transport safety (road and rail);

DIRECTORATE-GENERAL FOR MARITIME AFFAIRS AND FISHERIES (DGAMPA), for maritime transport safety;

### **5. Environmental protection:**

General Inspectorate for the Environment and Sustainable Development (IGEDD);

### **6. Radiation protection and nuclear safety:**

Nuclear Safety Authority and Radiation Protection (ASN);

### **7. Food safety:**

High Council for Food, Agriculture and Rural Areas (CGAAER);

National Agency for Food, Environmental and Occupational Health Safety (ANSES);

### **8. Public health:**

National Agency for Food, Environmental and Occupational Health Safety (ANSES);

National Public Health Agency (Santé publique France – SpF);

High Authority for Health (HAS);

Biomedicine Agency (Agence de la Biomédecine – ABM);

French Blood Establishment (EFS);

Committee of Compensation of Victims of Nuclear Tests (CIVEN);

General Inspectorate of Social Affairs (IGAS);

National Institute of Health and Medical Research (INSERM);

National Council of the Order of Physicians, for the practice of medicine;

National Council of the Order of Physiotherapists, for the practice of the profession of physiotherapist;

National Council of the Order of Midwives, for the practice of midwifery;

National Council of the Order of Pharmacists, for the practice of the profession of pharmacist;

National Council of the Order of Nurses, for the practice of the profession of nurse;

National Council of the Order of Dental Surgeons, for the practice of the profession of dental surgeon;

National Council of the Order of Chiropodists and Podiatrists, for the practice of the profession of chiropodist and podiatrist;

National Council of the Order of Veterinarians, for the practice of the profession of veterinarian;

### **9. Consumer protection:**

DIRECTORATE GENERAL FOR COMPETITION, CONSUMER AFFAIRS AND FRAUD CONTROL (DGCCRF);

### **10. Protection of privacy and personal data, network and information system security:**

National Commission for Information Technology and Civil Liberties (CNIL);

National Agency for Information Systems Security (ANSSI);

### **11. Violations affecting the financial interests of the European Union:**

French Anti-Corruption Agency (AFA), for breaches of integrity;

Direktorate General of Public Finances (DGFIP), for value added tax fraud;

Direktorate-General of Customs and Indirect Taxes (DGDDI), for customs duty, anti-dumping duty and similar fraud;

**12. Violations relating to the internal market:**

Direktorate General for Competition, Consumer Affairs and Fraud Control (DGCCRF), for anti-competitive practices;

Competition Authority, for anti-competitive practices and state aid;

Direktorate General of Public Finances (DGFIP), for corporate tax fraud;

**13. Activities conducted by the Ministry of Defence:**

General Audit Office of the Armed Forces (CGA);

College of Inspector Generals of the Armed Forces;

**14. Public statistics:**

Public Statistics Authority (ASP);

**15. Agriculture:**

General Council for Food, Agriculture and Rural Areas (CGAAER);

**16. National education and higher education:**

National and Higher Education Ombudsman;

**17. Individual and collective labour relations, working conditions:**

General Directorate of Labour (DGT);

**18. Employment and vocational training:**

General Delegation for Employment and Vocational Training (DGEFP);

**19. Culture:**

National Council of the Order of Architects, for the practice of the profession of architect;

Council of Auction Houses, for public auctions;

**20. Rights and freedoms in relations with State administrations, local authorities, public institutions and bodies entrusted with a public service mission:**

Defender of Rights;

**21. Best interests and rights of the child:**

Defender of Rights;

**22. Discrimination:**

Defender of Rights;

**23. Ethics of persons engaged in security activities:**

Defender of Rights.