DERICHEBOURG GROUP WHISTLEBLOWING POLICY

April 2024

DERICHEBOURG

SUMMARY

MESSAGE FROM THE CHAIRMAN AND CHIEF EXECUTIVE OFFICER

"Unethical behaviour has no place in our company. With your vigilance, we have no doubt that we will succeed in promoting a culture of responsibility and transparency at Derichebourg."

Abderaman El Aoufir

Chief Executive Officer of Derichebourg Environnement

Thomas Derichebourg

General Manager of Derichebourg Environnement

LEGAL FRAMEWORK

- This whistleblowing system is designed to meet the requirements of French law (which also apply to foreign subsidiaries, as the Derichebourg Group is a French Group):
  - The "SAPIN II" Act [1]
  - The Duty of Vigilance Act [2]
- The Group has appointed Corinne Belmont as Compliance Officer.
  - corinne.belmont@derichebourg.com
  - +33 1 44 75 43 33

[1] Law of 9 December 2016 as amended by the Law of 21 March 2022 – Articles 6 to 9, Article 17.II.2° – on transparency, the fight against corruption and the protection of whistleblowers
[2] Act of 27 March 2017 on the duty of vigilance of parent companies

WHO CAN SUBMIT A REPORT?

- A report can be submitted by any natural or legal person who has direct or indirect knowledge of specific facts or situations (see opposite). These include:
  - Employees;
  - Suppliers;
  - Customers;
  - Shareholders;
  - Corporate officers;
  - Trade unions;
  - Public bodies.

FOR WHAT REASONS CAN A REPORT BE SUBMITTED?

- Whistleblowing reports allow employees and third parties to report irregularities or shortcomings within the Group. A report may relate to the following subjects:


Corruption


Conflicts of interest


Fraud


Harassment

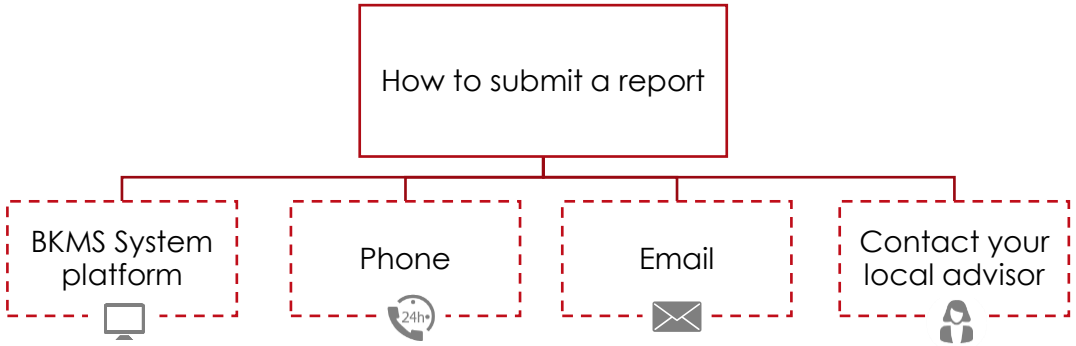
(sexual, physical, moral)


Discrimination / Racism


Working conditions


Environmental damage

HOW TO SUBMIT A REPORT



BKMS System online platform

The Derichebourg Group's whistleblowing system is an online platform accessible worldwide at:

https://www.bkms-system.com/Derichebourg-report

This link is available at all Group sites, along with an equivalent QR Code.

This is a highly secure system: neither the service provider nor any other third party has access to the data on the platform.

Reports submitted via the online system are visible to the Compliance Officer and the Control / Internal Audit department, which are obliged to respect your confidentiality.

Local contact person

Each Group subsidiary has a compliance contact person.
They have the authority to receive and process reports.
The list of local contact persons is available on the intranet

Phone

A telephone number is available in all countries where the Group operates:

Belgium	+32 289972611	**Mexico**	+52 5571002193
Canada	+1 2894019198	**Portugal**	+35 1304502651
France	+33 187212291	**Romania**	+40 317829807
Germany	+49 3099257146	**Spain**	+34 910477636
Hungary	+36 17011807	**Switzerland**	+41 435510235
Italy	+39 0281480081	**United States**	+1 2132791015
Luxembourg	+35 227860540		

To access the system, enter the following Company Access PIN: **2448**

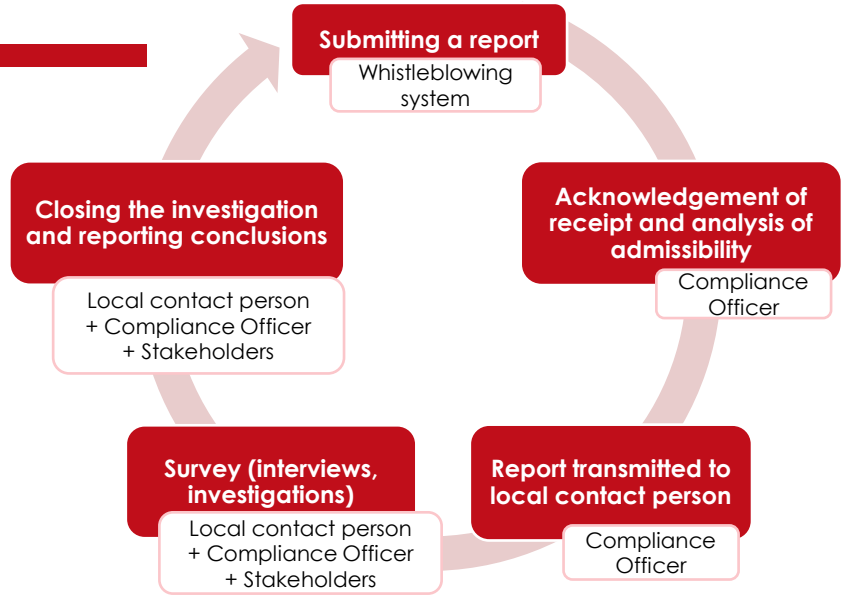
Mail

Reports may be sent by post to the following address:

Derichebourg Environnement
Compliance Officer - CONFIDENTIAL
119 Av. du Général Michel Bizot
75012 PARIS

However they choose to submit a report, the whistleblower can choose to remain anonymous

REPORT PROCESSING – OVERVIEW



For each alert transmitted, the Compliance Officer acknowledges receipt **within 7 working days**.

An analysis of admissibility is carried out collectively by the Compliance department within a period **not exceeding 3 months**. If the alert is deemed admissible, the whistle-blower is informed and the alert is forwarded to the relevant local contact, who is responsible for carrying out investigations. If the whistle-blower so desires, he or she may be contacted for further information. The person(s) in question may also be interviewed.

If the alert is deemed inadmissible, the whistleblower is informed, and the alert is closed.

In any event, the whistleblower will be informed of the measures envisaged or taken to assess the accuracy of the allegations and, if necessary, to remedy the subject of the alert, as well as the reasons for these measures, within a maximum period of 3 months.

At the end of the investigation, a report is drawn up.

WHO PROCESSES REPORTS?

Reports are received by the Compliance Officer, who directs them to be processed by the local contact persons in collaboration with the Compliance Officer.

However, the Compliance Officer is responsible for:

- Reports involving one or more members of management in a given country;
- Reports for which a particular circumstance (e.g., a conflict of interest) prevents unbiased or impartial processing at a local level

Investigation report

Once the report has been investigated, the local contact person draws up an investigation report presenting their conclusions as to the existence of conduct or situations violating the anti-corruption code of conduct, the ethics charter or the law. This report establishes the facts and, if possible, the responsibilities of those involved.

Whenever possible, the whistleblower is informed of the conclusions of the investigation report. The same applies to accused persons, if their identities were revealed in the report.

Group and subsidiary management are informed of investigations into the most sensitive situations. If the report establishes the existence of conduct / situation violating the anti-corruption code of conduct, ethics charter or legislation, Group and subsidiary management decide on any disciplinary and / or legal action to be taken against the employees / third parties involved.

Note: Investigation reports are formalised only in cases of fraud / corruption / conflict of interest

CONFIDENTIALITY AND TRANSPARENCY

- Confidentiality is key to the whistleblowing system, in order to protect the data collected and the identities of stakeholders.
- Local contact persons act under the aegis of the Compliance Officer. Information is collected and processed in accordance with the principles of proportionality and consistency, depending on the report.

It is imperative that the following two successive steps be followed:

1) The report is sent through one of the channels described in this policy;
2) If the whistleblower does not receive a reply from the Compliance Officer within the specified deadline, they may contact any external authorities.

WHISTLEBLOWER PROTECTION

- If submitted in accordance with the provisions of the Whistleblowing System, the report protects the following natural and legal persons:
  - the whistleblower;
  - facilitators, i.e., any natural or legal person who helps the whistleblower make a report or public disclosure;
  - any individual in contact with the whistleblower;
  - any legal entity controlled by the whistleblower.
- The Whistleblowing System stipulates that:
  - persons who have reported or publicly disclosed information in accordance with this policy are not civilly liable for damages caused by their reporting or public disclosure;
  - persons who have reported or disclosed information in accordance with this policy are not criminally liable;
  - individuals may not be subjected to retaliation or threatened or attempted retaliation.

It is recalled that a whistleblower who makes allegations they know to be false, with the intention of harming others or obtaining financial compensation, cannot be considered as "acting in good faith" and is therefore liable to prosecution for slander and libel under the law.

DATA RETENTION

- If the alert is inadmissible (i.e. no further action is taken as it does not fall within the scope of the procedure): destruction is possible but not compulsory. Data may be consulted on an ad hoc basis by specifically authorized persons. Such retention must meet an identified need, such as protecting witnesses from reprisals or providing evidence.

- If the alert is admissible and followed by an internal investigation: data relating to the alert may be kept until a final decision is taken. This decision must be taken within a reasonable time of receipt of the alert. Once the final decision has been taken on the action to be taken on the alert, the data may be kept in archive form, in particular for evidentiary purposes with a view to an audit or legal proceedings, or to carry out quality audits of the processes for handling alerts.

GENERAL DATA PROTECTION REGULATION (GDPR)

The Alert Device complies with the provisions of the General Data Protection Regulation (RGPD).

Only the following categories of data are recorded for the purposes of alert processing:

- identity, functions and contact details of the Author of the alert;
- identity, functions and contact details of the persons who are the subject of an alert;
- identity, functions and contact details of persons involved in collecting or processing the alert;
- facts reported;
- information gathered to verify the facts reported;
- report on verification operations;
- action taken on the alert.