

Group ***Internal***
Reporting System
Policy



I. Scope of application and addressees: This procedure is applicable to the DB Cargo Iberia Group. In this document, DB Cargo Iberia Group means both the group of companies as a whole and each of them individually.

The addressees are the members of the board of directors or administrative bodies, employees, managers, trainees (hereinafter, “employees”) and any other third party that uses the Internal Reporting System of the DB Cargo Iberia Group.



II. Basic principles and Internal Reporting Channels: The Internal Reporting System constitute a direct, efficient and confidential mean to file and manage reports on breaches of current legislation, internal regulations, the Code of Conduct of the DB Cargo Iberia Group or any fact of a similar nature by employees or collaborators of the DB Cargo Iberia Group as well as by any other third party (suppliers, customers, public administrations, shareholders, former employees, candidates in selection processes, etc.).

Potential users of the Internal Reporting Channels will be proper and clearly informed, in an easily accessible way, about the Internal Reporting Channels implemented by the DB Cargo Iberia Group, as well as about its essential management principles. Said information is available on the corporate website, through internal communication media and is actively transmitted to both employees, suppliers and other third parties through training, specific communications, contractual documents or accreditation processes.

Reports may be received through the following Internal Reporting Channels:

By e-mail to compliance@dbcargoiberia.com (whose recipients are the members of the Committee Responsible for the Internal Reporting System) or orally, by means of a face-to-face or online meeting upon request by the reporting person to the Compliance department of the DB Cargo Iberia Group.

In all cases, the report may be filed anonymously, although for the success of the investigation it is recommended that the reporting person indicate an address, email or safe place in order to maintain communications and receive requests for further information. Internal reporting channels should be the preferred channel for reporting legal or regulatory breaches, provided that the breach can be addressed effectively internally and where the reporting person considers that there is no risk of retaliation.



III. Committee Responsible for the Internal Reporting System

The Committee Responsible for the Internal Reporting System of the DB Cargo Iberia Group (hereinafter, Committee) is made up of the following members:

- Managing Direct
- Head of Legal, Insurance and Compliance
- Head of HR

The secretary of the Committee shall be the Compliance manager, to whom the Committee delegates the management of the Internal Reporting System and the processing of investigation files. The Secretary of the Committee will keep a confidential record book of every report received and the internal investigations resulting from these reports.

This record will not be public and may only be partial or totally disclosed to the competent judicial authority upon a reasoned decision request within the framework of a legal proceeding, and under the guardianship of that authority.

In the event that the report is filed through an Internal Reporting Channel operated internally, the Compliance manager will manage and review the report received. In either case, the Committee Responsible for the Internal Reporting System will decide whether to open an investigation. Such an investigation may be carried out either internally or externally.

The Committee Responsible for the Internal Reporting System will carry out its functions independently and autonomously from the rest of the group's bodies.



IV. Internal reporting procedure

A. First stage



1. Reports received

These are reports received through the channels mentioned in section II. previous.

When a report is received, the secretary of the Committee will carry out a preliminary analysis based on the type of report, its conditions, content, nature, credibility and possible parties involved. The secretary of the Committee will inform on the report and the results of the preliminary analysis to the Committee or part of its members based on the content of the report and any possible conflicts of interest that may exist (see the following section).

In both cases, an acknowledgment of receipt will be sent to the reporting person within 7 calendar days of that receipt, unless the confidentiality of the report may be endangered, together with information regarding the procedures for reporting externally to competent authorities.



2. Management of conflicts of interest for Committee members

If the secretary of the Committee is involved in a report, it will be communicated by the person who received it to the rest of the unaffected members of the Committee.

If a member of the Committee other than the secretary is involved in a report, it will be communicated to the other unaffected members of the Committee.

The person on whom the conflict of interest falls will not participate in the internal reporting procedure. When despite not being directly affected by the report, any of the members of the Committee considers that a conflict of interest affects them, they must inform the rest of the members and refrain from participating in the internal reporting procedure.

B. Second stage

This stage is common to every internal reporting channel.

Once the report has been received and once it has been managed and reviewed as indicated for the first stage, the Committee Responsible for the Internal Reporting System will determine:

- If an investigation is to be opened.
- If an investigation is not going to be opened: in cases in which the report is manifestly unfounded. The decision and the reasons therefor must be properly recorded. Such a decision shall not impede the initiation of a subsequent investigation if additional information is received at a later date.

The data may only be accessed by persons for whom this is essential for investigating the facts reported.

If the need to start the investigation process is agreed, the Committee will appoint an investigator (internal or external), who will carry out the investigations it deems necessary to clarify the issues reported.

The investigator will issue a confidential report that will contain, as a minimum:

- the reported facts,
- the results of the investigations and
- conclusions and recommendations.

The Compliance Manager shall submit the result of the investigation, together with a proposal for preventive and/or corrective measures – where appropriate – to the Committee, who shall formally approve the final measures to be adopted. Such persons may only access any personal data contained in the documentation or information relating to the report when this is necessary for adopting disciplinary measures or for processing judicial procedures.

Whenever possible, feedback on follow-up of the report will be provided to the reporting person.

The report containing the result of the investigation shall be filed together with the documentation relating to the investigation and kept by the Compliance Manager, outside the Internal Reporting System or channel. Personal data related to information received and internal investigations will only be kept for the period that is necessary and proportionate in order to comply with legal obligations. In no case may the data be kept for a period of more than ten years.

The Committee will report to the Management Body about the reports received, the course given to them, the compliance risks identified and the mitigating actions implemented or, where appropriate, the proposal of mitigating actions to be implemented.



V. Confidentiality of reports, good faith, protection of the reporting person and the persons concerned



A. Confidentiality

The Internal Reporting System is designed, established and managed in a secure manner, and guarantees the confidentiality of the identity of the reporting person and of any third party mentioned in the report, as well as of the actions carried out in its following-up, preventing access by unauthorized personnel.

Compliance with the applicable regulations regarding personal data protection, respect for the fundamental rights of the concerned persons and current labor legislation is guaranteed.



B. Reports in good faith

The principle of good faith shall apply in all reports made through any of the channels made available to employees and third parties outside the organization. The reporting person is deemed to act in good faith when the report refers to facts contravening the internal regulations, the Code of Conduct or applicable legislation and there are reasonable grounds to believe that the information is true.

On the other hand, the reporting person is deemed not to act in good faith when he/she is aware that the reported facts are untrue, acted in reckless disregard of truthfulness or with the intention of harming another employee. If bad faith in the reported information is proven, disciplinary measures may be imposed or, alternatively or jointly, court action may be taken against the reporting person.



C. Reporting person protection

The DB Cargo Iberia Group expressly prohibits any form of retaliation (including threats of retaliation and attempts of retaliation) against reporting persons who report in good faith an allegedly illegal act or facts allegedly contravening the internal regulations, the Code of Conduct or applicable legislation.

Likewise, it prohibits retaliation against a) the legal representatives of the employees when advising and supporting the reporting person, b) natural persons who assist a reporting person in the reporting process in a work-related context, c) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context (such as colleagues or relatives) and d) legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context, as well as against e) persons who publicly disclose breaches in accordance with Title V of Law 2/2023, regulating the protection of people who report on regulatory violations and the fight against corruption.

For the purpose of this policy, retaliation means any act or omission prohibited by law, or that have the direct or indirect effect of unfavorable treatment that puts the reporting person in a particular disadvantage with respect to others in a work-related context only because of their status as reporting persons or for having publicly disclosed a breach.

Retaliation includes in particular the suspension, dismissal or lay-off of the employment relationship, including failure to renew or early termination; cancellation or early termination of a contract for goods or services; imposition of any disciplinary measure; demotion or withholding of promotion and any other substantial modification of working conditions, etc.

The above measures will not be considered as retaliation when they are carried out within the regular exercise of the power of management under the labor legislation and due to circumstances, facts or proven infringements unrelated to the filing of a report.

Other examples of possible retaliation are for instance, harm, including to the person's reputation, or financial loss; coercion, intimidation, harassment or ostracism; negative performance assessment or employment reference; blacklisting or dissemination of information within a sector or industry which may hinder or prevent access to employment or recruitment; withholding of training; discrimination, disadvantageous or unfair treatment.

Any person who considers having suffered some type of retaliation due to a report or public disclosure made by them or by any person related to them, may request protection both through Internal Reporting Channels or through the independent whistleblower protection authorities (AAI and regional authorities).



D. Protection of persons concerned

During the following-up of a report, the persons concerned will fully enjoy the presumption of innocence, the right of defence and the right of access to the file, provided that the success of the investigation is safeguarded. They will also enjoy the same protection established for reporting people, that is the preservation of their identity and the guarantee of confidentiality of the facts and data of the procedure.



VI. Doubts and questions

In case of doubt, please get in touch with the Compliance department of the DB Cargo Iberia Group at the following address: compliance@dbcargoiberia.com



VII. Personal data protection

The processing of personal data derived from the management of the Internal Reporting System of the DB Cargo Iberia Group will be carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, with Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights and in Law 2/2023 on the protection of people who report on regulatory violations and the fight against corruption.

Personal data that is not clearly relevant to the processing of specific information will not be collected or, if collected accidentally, will be deleted without undue delay.

The Committee Responsible for the Internal Reporting System shall handle the data with absolute confidentiality, safeguarding the rights and freedoms of the interested parties.

The legal basis for processing personal data received through the Internal Reporting Channel is compliance with a legal obligation, in the terms laid down in article 6.1.c) of Regulation (EU) 2016/679 and in article 8 of Organic Law 3/2018. Employees and third parties will be informed about the processing of personal data within the framework of the Internal Reporting System of the DB Cargo Iberia Group. The reporting persons will also be expressly informed about the confidentiality of their identity, which will not be disclosed to the persons concerned by the report or to third parties, except to the competent judicial or administrative authority or the Public Prosecutor's Office within the framework of a criminal, disciplinary or sanctioning investigation and prior notice to the reporting person (unless said information could compromise the investigation or legal proceedings).

The personal data processed shall be kept in the Internal Reporting System only for the time required to decide on the appropriateness of initiating an investigation regarding the reported facts and it will be deleted at most three months after receipt of the report if an investigation has not been initiated, unless the purpose of conservation is to leave evidence of the functioning of the System. Reports that have not been processed can only be recorded anonymously.

The personal data processed in the framework of investigations will also be deleted from the Internal Reporting Channel within a maximum period of three months. It can be kept outside the channel for the time needed to investigate the facts and close the file and, once closed, they can be kept duly blocked as long as potential liability could arise from the reports or actions carried out by the DB Cargo Iberia Group.



Appendix 1: Insurance and Compliance Companies adhering to the Internal Information System Policy

- Company Date of adherence Administrative body that formalised adherence
- MDL Distribución Logística, S.A. 20 June 2016 Joint administrators
- Compañía Aragonesa de Portacoches, S.A. 20 July 2016 Board of directors