List of content

1 Purpose and goal 2
2 How you can reach us 2
3 Approach and responsibilities 2
3.1 Data protection, informant protection and confidentiality 2
3.1.1 Appointment of the investigation team 2
3.1.2 Handling of false information 3
3.2 Protection of the accused 3
3.3 Stages of the process 3
3.3.1 Acknowledgement and preliminary analysis 3
3.3.2 Investigation with the investigative team 4
3.3.3 Report of conclusions 4
3.4 Circumstances that indicate a criminal offense 4
3.5 Processing deadlines for compliance cases 4
4 Documents 5
5 Records 5
6 List of changes 5

1 Purpose and goal

The purpose of this document is to provide guidance to those who wish to report information about potential irregularities within the company. It procedure details how the process is carried out, the basic principles, the rights of the informant, how we deal with these reports, and how we communicate in such cases.

2 How you can reach us

To obtain information about events that direct, indirect employees, or other interested parties[1] believe are or may be material to the company, the following channels exist to report this information to the local or global compliance officer:

- Whistleblower app (see Menshen website: www.menshen.com)
- Compliance email address (compliance@menshen.com)
- Telephone (directly to the Compliance Officer)
- Letter (to the attention of the Compliance Officer)

These allow the transmission of this information to the local Information System Manager, which at Menshen is assumed by the local Compliance Officer and the investigation team assigned to each case. We expressly point out that, apart from the reporting channels mentioned above, there is the option of contacting the responsible authorities[i] directly (see "List of External Information Channels at the end of this document").

3 Approach and responsibilities

All reported potential compliance cases are processed by the Information System Manager at the respective location. This person is also responsible for ensuring that all reports are recorded in the compliance report and reported to the Compliance Officer of the Menshen Group.

3.1 Data protection, informant protection and confidentiality

Our reporting channels ensure that only those responsible for receiving and processing incidents and those who support them in completing the task(s) have access to incoming incidents.

The Information System Manager ensures the confidentiality of the identity of the following people:

- the person providing the information
- the person(s) who are the subject of an incident
- other person(s) named in the report

3.1.1 Appointment of the investigation team

The Information System Manager entrusted with processing an incident is responsible for and ensures that the identity of the aforementioned persons is known only to them or to the designated personnel for that case. External personnel must sign a confidentiality agreement along with the relevant contract as authorized collaborators for handling data from the Internal Information System. Internal personnel tasked with this duty must sign the acceptance of their appointment as stewards of the Menshen Iber Internal Information System.

[1] (i) employees; (ii) self-employed individuals; (iii) shareholders, participants, and members of the administrative, management, or supervisory body of a company; (iv) staff of contractors, subcontractors, and suppliers; and even (vi) volunteers, interns, and trainees, with or without compensation.

The requirement of identity confidentiality applies regardless of whether the Information System Manager is responsible for the incoming incident.

The Compliance Officer in their function is independent of all organizational units within the company and is not subject to the direction of the General Manager, ensuring that incoming reports are investigated impartially. If the Compliance Officer determines that they cannot act impartially in a particular case, they will inform the Mensheen Group Compliance Officer and request that they lead the investigation.

3.1.2 Handling of false information

If an allegation is made based on a genuine, albeit erroneous, belief in wrongdoing, the informant remains protected by the whistleblower system, and no sanctions will be imposed after the facts have been clarified.

If it turns out that the allegation was intentionally false and malicious, we reserve the right to take appropriate action against the informant. For an internal informant, this could result in labor law-related and/or criminal law-related consequences, and for an external informant, criminal law-related consequences.

3.2 Protection of the accused

In principle, everyone who is implicated and under investigation of a potential compliance incident is subject to the presumption of innocence. When processing a compliance case, it must be ensured that the protection of personal data is guaranteed. Furthermore, the person investigated has the right to be informed of the actions or omissions with which they are accused and to be heard at any time.

If the clarification of the facts reveals that the accused person was falsely suspected, we will officially exonerate the accused from the allegations. The exoneration will be provided in writing.

If the accused individual has potentially suffered internal or external harm as a result of the false accusations, we will take internal and/or external communication measures to clarify that the allegations were unfounded.

3.3 Stages of the process

3.3.1 Acknowledgement and preliminary analysis

If the person providing the information identifies themselves with their contact details, they will receive feedback from the Information System Manager that the report has been received. After a preliminary analysis, the Information System Manager will inform the informant whether their report is archived and the case closed, or if an investigation is opened, having the opportunity to clarify any queries that may arise during processing in direct contact.

This is not possible for reports that reach us anonymously, except when using the whistleblower app (in the App only indirectly). If the informant uses the app, they can save the report number. A corresponding note is given when entering the message. This message number can be entered into the app at any time to monitor the status of processing or to provide further information.

If the Information System Manager has any questions while processing an incident that have reached us via the app, they can document them in the App. However, it is not possible to determine whether these are read by the information provider, as the app ensures that all entries made cannot be traced back.

If information about a possible compliance incident reaches the company via those who are not officially entrusted with processing compliance incidences, the procedure will be as follows:

The Information System Manager informs the person concerned that they are obliged to maintain absolute secrecy about this knowledge. The person instructed in this regard must sign the protocol drawn up for this conversation by the Information System Manager. Thus, they are warned that failure to comply with the confidentiality obligation is classified as a very serious offense. If there is a violation of the instruction to maintain confidentiality, this will have consequences under labor law.

3.3.2 Investigation with the investigative team

The investigation of a complaint case consists of a structured and confidential process to examine the reported allegations. This process begins with an assessment of the allegation by the manager together with the designated investigative team to determine its veracity and seriousness. Relevant evidence is then gathered through interviews, document review, and other investigative techniques. The objective is to clarify the facts, identify possible violations, and determine whether internal policies or applicable laws have been violated. Throughout the process, the whistleblower is guaranteed protection against retaliation and the confidentiality of information is maintained.

3.3.3 Report of conclusions

At the end of the investigation, a detailed report is prepared with the findings and recommendations for decision making and, if necessary, the implementation of corrective or disciplinary measures. This report of findings is given to the Human Resources Manager and submitted to management. The report includes a summary of the complaint, analysis of the evidence gathered, interviews conducted, and any relevant documentation. It also details the conclusions obtained and suggests concrete actions to resolve the irregularities identified. The Human Resources Manager reviews the report and coordinates with the management team to decide on the actions to be taken, ensuring that all internal policies and applicable laws are complied with. Management evaluates the recommendations and, if necessary, orders the implementation of corrective or disciplinary measures, as well as the implementation of changes in internal processes to prevent future irregularities. The entire process is meticulously documented to ensure transparency and accountability in the handling of the complaint.

3.4 Circumstances that indicate a criminal offense

If, during the processing of a compliance matter, evidence emerges that point to a criminal offense, the responsible public prosecutor's office will be informed by the Compliance Officer.

3.5 Processing deadlines for compliance cases

The following deadlines apply to the processing of compliance issues:

- The Information System Manager must confirm the receipt of the note in writing to the individual providing the information no later than 7 calendar days after receipt.
- The investigation of each compliance case must be started not later than 15 calendar days after receipt of the information. The local Information System Manager is responsible for documenting the receipt of the information and the start of the investigation with the date and, if possible, the time of the transaction.

- Each compliance incident must be addressed within three months. Exceptions can be made in complex cases. In such cases, the processing time can be extended an additional three months.

The informant will receive written feedback within three months. The feedback includes the notification of the status of your complaint or communication: whether it has been filed, whether an investigation has been opened, whether the investigation is still ongoing, or whether the investigation has been completed, action has been taken and the case has been closed.

4 Documents

- M01_PI_03_Compliance-Management_INT

5 Records

- Compliance Notes
- NDA external managers of the Internal Information System
- Contract for External Manager in charge of Internal Information System Data Processing
- Letter of Acceptance Internal Managers

6 List of changes

Date	Index	Description of the change
2025-11-17	B	• 3.1 Data protection, informant protection, confidentiality and impartiality was 3.1 Data protection, informant protection and confidentiality • 3.1.1. Appointment of the investigation team 3. paragraph added • 3.1.2 Handling of false information chapter added • 3.2 Protection of the accused 2. and 3. paragraph added

[i] List of External Information Channels

- Oficina Europea de Lucha contra el Fraude Unión Europea (OLAF:

https://fns.olaf.europa.eu/main_es.htm

- Fiscalía Europea (EPPO):

https://www.eppo.europa.eu/es/form/eppo-report-a-crime

- Autoridad Independiente de Protección del Informante (AAI):

Pendiente de creación del canal

- Servicio Nacional de Coordinación Antifraude (SNCA):

consultasantifraude@igae.hacienda.gob.es

- Oficina Antifraude de Cataluña (OAC):
- Buzón antifraude - Canal de denuncias del Mecanismo para la Recuperación y Resiliencia

https://planderecuperacion.gob.es/buzon-antifraude-canal-de-denuncias-del-mecanismo-para-la-recuperacion-y-resiliencia