WHISTLEBLOWING SYSTEM PROCEDURE

COMPLIANCE

May 2022

General introduction

Mersen has a proprietary whistleblowing system that enables concerned employees to report:

- any conduct or actions defined as inappropriate by the Group's Code of Ethics;
- a crime or offense;
- a serious and manifest breach of an international commitment duly ratified or approved by France;
- a serious and manifest breach of a unilateral act by an international organization that is based on a duly ratified international commitment;
- a serious and manifest breach of the law or regulations;
- a serious threat or harm to the public interest, of which the whistleblower has become personally aware.

This system is intended for all Mersen Group employees and external or temporary human resources.

Mersen Group employees and external or temporary human resources who do not wish to use it can employ other methods of reporting.

Whistleblowers who use the system in good faith do not risk any disciplinary measures, even if their allegations are not substantiated or do not lead to any further action. In contrast, whistleblowers who misuse the system with allegations that are not in good faith, such as by giving false or incorrect information on purpose or with malicious intent, can face disciplinary and legal action.

Data controllers and purposes

Mersen Corporate Services and each Group company employing employees are jointly responsible for the processing of personal data carried out for the purposes of managing the whistleblowing system.

We remind you that the Code of Ethics and the Anti-Corruption Code are available on the Group Intranet.

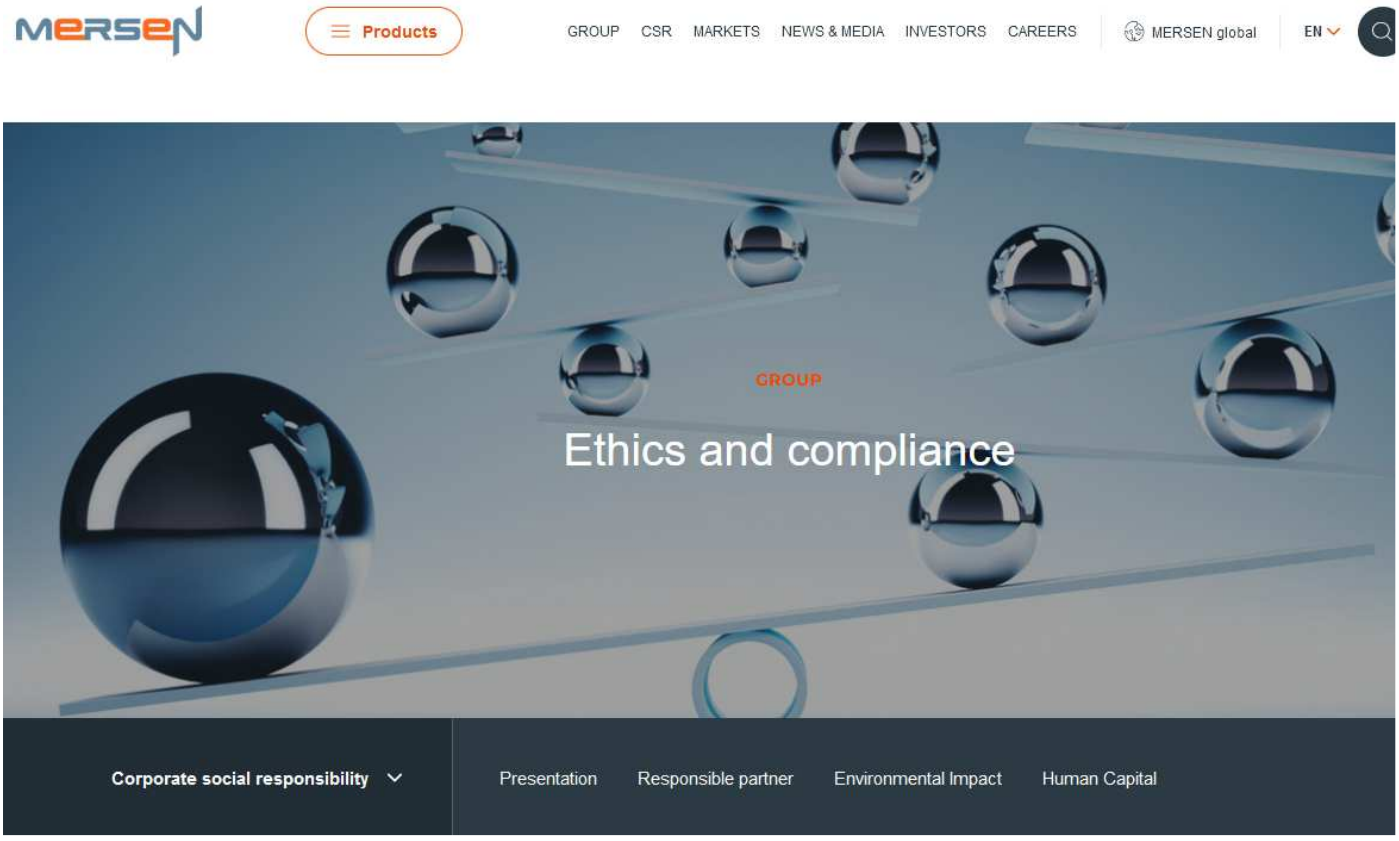
Whistleblower report collection and processing

Reports can be submitted through two main channels:

1) By sending an email to the system: ethics@mersen.com
2) By completing a form on the mersen.com website

https://www.mersen.com/group/whistleblowing-contact-form

This form is available in the CSR section of the Group's website (mersen.com).



Both channels send reports to the following two email accounts only:

- The Group Vice President of Human Resources
- The Group Compliance Officer

Note:

In both cases, an email is automatically sent to the whistleblower to confirm that their request has been received and will be handled.

Whistleblowers can identify or not themselves. If identity is revealed people responsible for the system will treat identity as confidential.

In some cases, whistleblowers can remain anonymous but the way their report will be handled will depend on whether:

- the seriousness of the allegations is established, and the facts are known in enough detail;
- any special precautions will need to be taken when handling such reports: for example, the initial recipient will first have to assess whether it is advisable to transmit the report using the system.

In addition to the aforementioned recipients, the data collected will only be accessible by the judicial authorities in the event of a report.

It is specified that, in accordance with the legal or regulatory provisions which strictly frame the communication of information, the elements likely to identify the issuer of the alert can only be disclosed, except to the judicial authority, with the consent of the person. Likewise, the elements likely to identify the person implicated in an alert may not be disclosed, except to the judicial authority, once the base of the alert has been established.

Whistleblower report handling

When a report is received, the Group's Vice President of Human Resources and Compliance Officer meet to jointly decide whether further action should be taken.

An investigation is always launched with the assistance of local representatives, who are generally the location's HR and/or its General Manager. If the report concerns HR or the General Manager, the investigation is carried out with other local representatives.

The people responsible for collecting and handling whistleblower reports are under a heightened obligation to protect confidentiality.

Only the following categories of data can be processed:

- the identity, responsibilities and contact information of the whistleblower;

- the identity, responsibilities and contact information of the people who are the subject of a whistleblower report;
- the identity, responsibilities and contact information of people involved in collecting or handling the report;
- the allegations;
- the facts collected to verify the allegations;
- the record of verification activities;
- further action taken in response to the whistleblower report.

Once the investigation is complete and its findings have been discussed with local management, the Group's Vice President of Human Resources and Compliance Officer decide whether further action should be taken.

The following are examples of possible cases where no further action is taken after investigating a whistleblower report:

- an alert has clearly been made as an act of revenge for various circumstances such as employee dismissal or professional jealousy;
- there are no findings to justify the alert.

If a report is justified, the Compliance Committee, consisting of the Group's CEO, CFO, Vice President of Human Resources and Compliance Officer, meets to consider the decision to be made and any potential disciplinary measures to be taken.

Data related to a report that, upon being received by the person responsible for handling it, are deemed to fall outside the system's scope are destroyed or redacted for anonymity and archived.

If a report does not lead to disciplinary or legal proceedings, the data related to the report are destroyed or redacted for anonymity and archived within two months of the report being closed. The whistleblower and the person who is the subject of the report will be notified when the report is closed.

If disciplinary or legal proceedings are initiated against a person who is the subject of a report or who made a report in bad faith, data related to the report are stored until the proceedings have ended.

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

Alert Issuer Information

Persons who report via the device will receive processing information from the start of the alert gathering process.

An acknowledgment of receipt will be provided to the Alert Issuer to enable it to benefit, where appropriate, from a specific protection regime. This acknowledgment will be time stamped. It will summarize all of the information and, where applicable, the attachments communicated within the framework of the report. To respect the anonymity of the whistleblower who requests it, the delivery of this receipt will not be subject to the production of identifying information (email or postal address, etc.).

When a decision on the follow-up to the alert has been taken by the controller, the Alert Issuer will be informed.

Information of the person targeted by the Alert

The Person concerned by the Alert will be informed without delay of the facts, the subject of the Alert, in order 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 information of the Person targeted by the Alert will intervene after the adoption of these measures.

This information will specify in particular the facts that are alleged, the entity responsible for the device, the services possibly receiving the Alert as well as the procedures for exercising its rights of access and rectification.

Rights of persons concerned

The person responsible for the Alert device guarantees to any person identified in the internal alert device the right to access the data concerning him and to request, if they are inaccurate, incomplete, ambiguous or outdated, rectification or deletion.

Access Rights

Any person whose personal data is or has been processed in the context of a professional alert (Issuer of the alert, alleged victims of the facts, persons targeted by the alert, witnesses and persons heard during the investigation, etc.), has the right to have access to it.

The exercise of this right must not allow the person exercising it to access personal data relating to other natural persons. The person who is the subject of an Alert cannot in any case obtain communication from the controller, on the basis of his right of access, of information concerning the identity of the Issuer of the Alert.

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 of opposition cannot be exercised for processing necessary for compliance with a legal obligation to which the controller is subject.

It cannot therefore be exercised with regard to the processing set up by companies fulfilling the conditions of articles 8 and / or 17 of the law known as "Sapin law 2".

Rights of rectification and destruction

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 professional alert systems, it must in particular not allow retroactive modification of the elements contained in the alert or collected during its investigation. Its exercise, when admitted, should not result in the impossibility of reconstructing the chronology of any changes to important elements of the investigation.

This right can therefore only be exercised to rectify factual data, the material accuracy of which can be verified by the controller with supporting evidence, without erasing or replacing the data, even erroneous, initially collected.

The right to destroy is exercised under the conditions provided for in article 17 of the GDPR.

These rights can be exercised, at any time, by sending a letter by email to the following address: data-protection@mersen.com

Any person concerned may also, if they wish, lodge a complaint with the National Commission for Data Protection (CNIL for France) or any other body of this type in the country concerned.

Transfer of data outside the European Union

As Mersen Group operates in several different countries, your personal data may be transferred outside the European Union. The list of countries in which Mersen Group companies are located can be viewed on the website via the following link: https://www.mersen.com/

If certain third parties are in countries where local regulations do not provide the same level of protection as EU member states, Mersen Group will ensure that transfers are carried out in accordance with European regulations (e.g., by implementing the contractual clauses adopted by the European Commission).