www.emeis.com

Procedure for collecting and processing reports

Group

Procedure for collecting and processing reports
Group

Procedure for collecting and processing reports
Group

01. PURPOSE OF THE DOCUMENT

Within the context of *emeis*'s ongoing goal to strengthen its ethical commitments and offer easily accessible tools to anyone wishing to report a situation that is inappropriate or that does not comply with its principles or applicable laws and regulations, ***emeis*** **provides its employees and stakeholders with a Whistleblowing System.**

This System completes the existing channels and reinforces *emeis*'s Ethical Conduct approach. **It gives anyone wishing to report a situation an easy, confidential and, if necessary, anonymous way of doing so**.

The ethical whistleblowing system is by no means an emergency system and does not replace existing systems for reporting events that are an immediate threat to people or property. Using the Whistleblowing system is optional.

emeis has revised the existing Whistleblowing System and redefined the procedure in compliance with the European Directive on the protection of Whistleblowers of 23 October 2019 (hereinafter referred to as the "European Directive". In French law, the Waserman Law of 21 March 2022 transposes the European Directive, and the Decree of 3 October 2022 specifies its implementing rules.

Lastly, *emeis* does its utmost to ensure the security and confidentiality of data sent, including personal data that may be collected for the purpose of receiving and processing a whistleblowing concern.

This procedure applies to *emeis* S.A and to all of its subsidiaries in France. Thus, the rules described in this document are established in relation to French law.

02. SCOPE OF APPLICATION

The System implemented within *emeis* covers whistleblowing concerns relative to the following breaches and violations:

Breaches in relation to violation of the Anti-Corruption Code of Conduct (Article 17 of the "Sapin II" Law)

- The existence of conduct or situations that run counter to the Group's Anti-Corruption Code of Conduct, insofar as they are likely to be characteristic of acts of bribery or influence peddling.

Other breaches (Article 6 of the "Sapin II" Law)

- a crime, an offence;
- a threat or harm to public interest;
- a violation or attempt to conceal a violation of an international commitment duly ratified or approved by France, of a unilateral act of an international organisation made on the basis of such a commitment, of European Union law or of a law or regulation.

Risks of serious harm within the context of the Group's duty of care (Article 1 of the law called "duty of care" of 27 March 2017)

- The existence or realisation of risks of serious violations of human rights and fundamental freedoms (including discrimination, bullying and sexual harassment), the health and safety of individuals and the environment, resulting from the Group's activities or those of its sub- contractors or suppliers with which it maintains an established business relationship, when such activities are linked to this relationship...

Other breaches of the Group's Ethics and CSR Code of Conduct.

Procedure for collecting and processing reports
Group

03. WHO CAN MAKE A REPORT?

Internally

- Group employees
- former employees if the information that is the subject of the report was obtained within the context of this relationship
- candidates for employment if the nformation that is the subject of the report was obtained within the context of this relationship
- shareholders, partners and holders of voting rights at the general meeting
- members of the administrative,
- management and supervisory bodies
- Occasional employees

Externally

- External employees
- co-contractors and sub-contractors (suppliers, service providers, partners, etc.) or the members of staff and of the administrative, management or supervisory body of these cocontractors and sub-contractors

04. WHICH KINDS OF ACTS OR BEHAVIOURS CAN BE REPORTED?

Any breach of our ethical principles and all other violations of laws and regulations and any incidents involving, but not limited to, the following areas:

- **Bribery, influence peddling and conflicts of interest**
- **Discrimination, bullying and harassment, health and safety at work**
- **Fraud, misappropriation and theft**
- **Anti-competitive practice**
- **Individual rights and protection**
- **Environmental protection**
- **Non-compliance with laws, regulations or public interest**

Facts, information and documents relating to the care of patients or residents are not processed by this System and are subject to specific procedures at *emeis* via a listening platform www.emeis.com/plateforme-ecoute and/or a mediation facility www.emeis.com/dispositif-mediation

05. THE SYSTEM COORDINATOR AND THE PERSONS IN CHARGE OF RECEIVING AND PROCESSING REPORTS

The France Compliance department and the Compliance Corporate department are responsible for receiving and processing reports within their respective scope, and act as the Principal Alert Referent (PAR).

The PAR may call on other departments (Human Resources, Legal, Finance, IT, etc.) or external third parties based on their ability and their impartiality in conducting investigations, as part of the effective processing of an alert.

All persons in charge of receiving and processing a report are bound by a duty of confidentiality.

06. WHAT PROTECTION IS GIVEN TO THE WHISTLEBLOWER, FACILITATORS AND THE PERSONS INVOLVED?

National laws on the protection of Whistleblowers (Waserman Law) and the European Directive protect Whistleblowers from retaliations and sanctions.

However, **the author of the report must meet the following cumulative conditions in order to benefit from Whistleblower status**:

- **be a natural person** and not a legal entity (a company, an association or a trade union);
- **act without any direct financial compensation,** i.e. not expect to be paid for the report made;
- **act in good faith**, i.e. not act maliciously or with revenge by reporting information that they know to be false or misleading;
- **have knowledge of the facts** either in the professional context (the Whistleblower may report facts of which they have personal knowledge, or which have been reported to them) or outside the professional context (the Whistleblower must have had personal knowledge of the facts they are reporting); and
- **be identifiable:** the reporting platform is subject to the identification of the Whistleblower. Exceptionally, anonymity is permitted if the seriousness of the facts reported is established and if the facts are sufficiently detailed. The Whistleblower can only benefit from protection measures (see below) once anonymity has been lifted.

Protection of the Whistleblower's identity, which will not be disclosed

The System ensures strict confidentiality of the identity of the Whistleblower, the persons concerned and the information received, at every step of processing the whistleblowing concern. Elements to identify the Whistleblower:

- **can never be disclosed to the person involved in the alert,** even if they exercise their right of access under data protection law,
- **can always be disclosed to a judicial authority upon request,**
- can be disclosed, outside the judicial authority, **to anyone only after obtaining the Whistleblower's prior consent.**

Protection against possible retaliations

Subject to raising an alert in accordance with the provisions set down in this document, the Whistleblower cannot be the subject of retaliations, threats or attempts to use such measures, even if the facts subsequently prove to be inaccurate or do not give rise to any follow-up.

Criminal and civil protection (criminal and civil non-liability)

The Whistleblower cannot be held criminally liable if the report is necessary and proportionate to the protection of the interests involved.

Nor can the Whistleblower be held civilly liable in the event of damage caused by the report if they had reasonable cause to believe in the protection of the interests involved.

Other stakeholders

This protection also applies to:

- **facilitators,** defined as any natural person or non-profit legal entity under private law (trade unions and associations) which help a Whistleblower to make a report in compliance with the law,
- **natural persons linked to the Whistleblower** (colleagues and family),
- **legal entities controlled by the Whistleblower** for which they work or with which they are linked in a professional context (for example a third-party supplier or sub-contractor of which the Whistleblower is a director or employee).

If the aforementioned conditions are not met, the author of the report shall not benefit from protected Whistleblower status. However, even without Whistleblower status, **a report made in good faith shall not give rise to punitive measures.**

The Whistleblower must act in good faith, not deliberately make false accusations or have the sole intention to harm and to gain personal advantage. Any misuse or use in bad faith of the Whistleblowing System may result in disciplinary sanctions if the reporter is an employee, as well as possible legal proceedings.

07. INFORMING THE PERSON CONCERNED BY AN ALERT

The present system for handling professional alerts requires the processing of data relating to identified or identifiable individuals. Anyone who is the subject of a report qualified as admissible which becomes an alert (as a witness, victim or alleged offender, for example) must be informed of the processing of their data in the context of this purpose in application of the applicable regulations on the protection of personal data (GDPR and Data protection act), with the aim of transparency and in particular so that they can exercise their rights of access, opposition, rectification or deletion of data (see Appendix 1).

However, this information may be deferred if it is deemed necessary to adopt precautionary measures to prevent the risk of evidence being destroyed.

For reasons of confidentiality and to comply with data protection legislation, **the person involved in a whistleblowing concern may not, in any circumstances, obtain from *emeis*,** on the basis of their right of access, **information concerning the identity of the Whistleblower** or any other person involved in the investigation.

The identity of the person involved in an alert will be **handled in the strictest confide**nce. The elements that can identify them can only be disclosed once it has been established that the whistleblowing concern is well-founded (unless such information has to be communicated to the judicial authority).

08. MAKING AN ALERT

8.1 Whistleblowing channels

If they have obtained information within the context of their professional activity relating to facts that have occurred or are very likely to occur in the entity concerned, the Whistleblower may alternatively or cumulatively report the concern internally or externally:

Internally

In compliance with this procedure for collecting and processing reports (see 8.2 and 8.3 below).

Externally

In compliance with laws in force, the Whistleblower may also submit their alert, either after raising it internally, or directly:

- to the competent external authorities listed in the appendix of Decree No. 2022-1284 of 3 October 2022;
- to the Rights Defender, who will guide them to the authority or authorities best placed to deal with it;
- to the judicial authority;
- to a European Union institution, authority or body competent to collect information on breaches falling within the scope of the aforementioned Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019.

8.2 Internal whistleblowing

In practice, any alert can be addressed by the employee to their line manager (direct or indirect, unless they are involved) or via the whistleblowing platform described in this System.

Through the line manager

Through the Whistleblowing platform

If the line manager is contacted by an employee, their role is to guide and advise them and to encourage them to use the Whistleblowing System to contact the PAR.

emeis encourages all Whistleblowers to use the Whistleblowing Platform presented in Section 8.3 , in particular for the following reasons:

- **To maintain the confidentiality and security of communications;**
- **To ensure the effectiveness, traceability and continuity of whistleblowing management;**
- **To ensure transparency with regard to complying with the rules described in this Chapter;**
- **To protect the Whistleblower.**

If the report is made outside of the whistleblowing platform, it may be integrated into the whistleblowing platform by the recipient of the alert after informing the Whistleblower and respecting their anonymity if they so wish.

8.3 Alert internally using the whistleblowing platform

The alerts are transmitted via the platform available at the following address:

> emeis.signalement.net

Or

> by using the following telephone number: **01 86 47 77 67** and entering the code **1989**

The author of the report is requested to follow the steps below:

1. **select a whistleblowing category,**
2. **enter their contact details or remain anonymous,**
3. **describe the facts accurately and objectively,**
4. **if applicable, attach documents,**
5. **read through and transmit the report.**

When using the whistleblowing platform, the author of the report will be asked to classify their report in one of the categories mentioned in Section 4. This categorisation may be amended after it has been analysed by the PAR.

It is important to include as much information as possible (evidence, documents, etc.) when making a report to enable the PAR to analyse, process and investigate it as effectively as possible.

The investigations may be made more difficult, particularly if the PAR of the alert cannot collect additional information from an anonymous Whistleblower. Anonymity may also make it more difficult to establish the credibility of the allegations and the effectiveness of the protection granted to the Whistleblower. In any case, a Whistleblower who wishes to remain anonymous is invited to give the PAR the means to exchange with them in order to facilitate the investigation of the facts that led to the report.

Once the report has been written and transmitted on-line:

- **the platform automatically issues a secure confidential code to the author of the report.** This is their personal identifier which ensures the confidentiality and protection of the data transmitted. This code will be requested for each new connection to the report made in order to be able to consult the follow-up, make any amendments or reply and exchange with the person in charge of processing it.
- at the same time, **an automatic notification is sent via the platform to the PAR of the scope concerned**.

09. PROCESSING THE ALERT REPORTED ON THE INTERNAL CHANNEL

9.1 Acknowledging receipt of the report and informing the Whistleblower

From the time the report is filed, the PAR has a maximum of **7 days** in which to send a written acknowledgement of receipt to the author of the report. This messages states, among other things:

- **that the report has been received,**
- **the reasonable and foreseeable time** required to examine its admissibility (usually **30 days**, except in exceptional circumstances).

9.2 Analysing the admissibility of the report

The PAR makes an independent and objective examination of the admissibility of the report in order to decide whether it comes within the scope of the System.

The person author of the report may be requested to provide additional information to proceed with this analysis. Without a response from the person making the author of the report, or if the additional information communicated is unsatisfactory, the report shall be deemed non-admissible.

Reports deemed **non-admissible are closed for non-admissibility**.

Reports deemed **admissible are qualified as alerts and shall be investigated** (see 9.3 below).

The author of the report is informed within 30 days from the date of acknowledgement of receipt of the decision on **admissibility or non-admissibility** of their report.

9.3 Investigating the alert

Within the context of processing the alert, internal and external investigations will be conducted to determine whether the facts are true.

Depending on the alert, the PAR may:

- **process the alert directly** with support from competent persons in the *emeis* Entity or an external party;
- **delegate the alert** to a competent department.

The time period required to process an alert may vary depending on its complexity and the research and verifications that need to be carried out.

9.4 Closing the whistleblowing concern

The PAR will inform the Whistleblower and the persons involved in the alert of the outcome and conclusions and, if applicable, the measures taken.

The Whistleblower should be informed within three (3) months of acknowledgement of receipt of their report.

10. CONFIDENTIALITY

The PAR and the persons involved in the processing of the alert take **all appropriate measures to comply with applicable laws on data protection and medical confidentiality,** and to **preserve the confidentiality of information,** whether during collection, processing or storage/archiving.

All alerts shall be processed **in the strictest confidentiality** and shall not be disclosed to anyone other than the recipients authorised to receive or to investigate the concerns.

The recipients of the alert are subject to an **enhanced confidentiality obligation**.

Elements that can identify the Whistleblower **can only be disclosed with their consent** (unless this information has to be sent to a judicial authority).

Elements that can identify the person accused by the alert can only be disclosed once it has been established that the alert is well-founded (unless this information has to be sent to a judicial authority).

11. MONITORING AND STEERING

A Steering Committee to monitor alerts has been set up in France and meets monthly. Its role is to ensure the due implementation of this procedure. It has access to the reporting statements prepared by the PAR. These statements list whistleblowing concerns received and their state of progress.

This policy may be amended as needed by the Group Compliance department. These amendments may be made at any time to represent regulatory changes or to incorporate new details that are identified.

Initial version: 2018
Current version: 31 July 2023

APPENDIX 1: INFORMATION ON THE PROCESSING OF PERSONAL DATA

Data controller

The personal data collected is processed under the supervision of the data controller, which is *emeis* S.A. (12 rue Jean Jaurès, 92800 – Puteaux - France).

Purposes and legal bases of processing

The Whistleblowing System aims to collect and manage reports of conduct or situations that run counter to applicable laws and regulations, or an Ethics and CSR Code of Conduct.

This System is implemented by the Group in order to comply with the provisions of the Sapin 2 Law and the Duty of Care Law and, if applicable, for the legitimate purpose of enabling *emeis* and/or any of its subsidiaries to be informed and be in a position to act promptly and appropriately in the event of a violation of any applicable law or regulation.

Group legal obligation

This Whistleblowing System has been set up by the Group to comply with the provisions of the Sapin II law to enable "internal employees and external or occasional employees" of an organization, to report:

- a crime or an offence;
- a serious and manifest violation of an international commitment duly ratified or approved by France;
- a serious and manifest violation of a unilateral act of an international organization taken on the basis of a regularly ratified international commitment;
- a serious and manifest violation of the law or regulations;
- a serious threat or prejudice to the general interest, of which the issuer of the alert has personal knowledge.

This Whistleblowing System has also been set up by the Group to comply with the provisions of the French «Duty of care» law, and to enable the collection of alerts relating to the existence or realization of risks of serious violations of human rights and fundamental freedoms, the health and safety of individuals and the environment, resulting from the activities of the company and those of the companies it controls within the meaning of II of Article L. 233-16, directly or indirectly. 233-16, either directly or indirectly, as well as the activities of subcontractors or suppliers with whom we have an established commercial relationship, when these activities are linked to this relationship.

Legitimate interest pursued by the Group or by the recipient of the data

This Whistleblowing System is finally set up by the Group on a voluntary basis, outside of any specific legal obligation, to enable *emeis* and/or any of its subsidiaries to be informed and able to act promptly and appropriately in the event of a violation or suspected violation of any applicable legislation or regulation or code of conduct.

Personal data concerned

The data that may be processed as part of the *emeis* alert procedure is limited to the following information:

- identity, functions and contact details of the author of the report
- identity, functions and contact details of persons who are the subject of an alert
- identity, functions and contact details of persons involved in receiving and/or processing the alert
- facts reported
- elements collected to verify the facts reported
- report of verification operations
- further action carried out
- data revealing the state of health, racial or ethnic origin, religion, life and sexual orientation, political opinions or trade union membership: if processing of these data is necessary for the establishment, exercise or to defend a right in court
- information relating to offenses or convictions to which a person has been subject: if processing authorized by national law or to enable the Group to prepare, take and follow legal action as a victim, defendant, or on behalf of them

Data recipients

Personal data processed as part of the Whistleblowing System is only intended for authorized persons, namely:

- Internally: persons specifically responsible for managing alerts within the Group; PAR; steering committee for monitoring alerts (in France and at Corporate level)
- Externally: judicial authorities; subcontractor managing the alert management platform.

Transfer outside the European Union (EU)

The Group uses a subcontractor based in France to manage the professional whistleblowing platform, which is itself required to partially subcontract this service to a third party located outside the EU, whose staff are physically located outside the EU.

In order to provide a framework for this data transfer, and in compliance with the GDPR, standard contractual clauses have been concluded and ensure a level of protection for your personal data at least equivalent to that provided within EU countries.

Personal data storage periods

Personal data collected and processed within the context of the Whistleblowing System is stored only for the time strictly necessary for the intended purpose, as described below:

- If the report is deemed non-admissible (does not constitute an alert), the data is immediately destroyed or made anonymous.
- If the report is deemed admissible (constitute an alert) and closed without further action after investigation, the data is kept and deleted within two (2) months of the closure of the verification
- operations, then deleted or anonymized.
- If the facts resulting from the alert are established but do not give rise to disciplinary or legal proceedings, the data is stored for 6 (six) years and then deleted (or anonymized)
- If the alert is followed by disciplinary or legal proceedings against the concerned person or the author of an abusive alert, the data is kept until the end of the proceedings and until any appeals against the decision are time-barred.

Exercising rights relating to personal data processing

Pursuant to Articles 15 et seq. of the GDPR, any Data Subject whose personal data is collected and processed via the Whistleblowing System is entitled to request from *emeis*, or any of its subsidiaries when the report is issued by a member of its staff or one of its external collaborators, or when the facts reported concern the said subsidiary, access to their personal data, rectification thereof and, if the conditions are met, deletion thereof, as well as a restriction on its processing, the right to object the said processing and the right to the portability of their personal data.

Lastly, pursuant to the French Data Protection and Civil Liberties Law, any Data Subject has the right to define instructions for the conservation, deletion and communication of their personal data after their death.

Any Data Subject can exercise their rights by writing to the following e-mail address: dpo@emeis.com, specifying their request and including proof of identity. This request can also be made by writing to the following postal address: *emeis* – Data Protection Officer, 12 rue Jean Jaurès, CS 10032, 92 813 Puteaux Cedex.

Any person may also lodge a complaint with the Commission Nationale de l'Informatique et des Libertés ("Cnil") at the following address: 3 place de Fontenoy - TSA 80715 - 75334 Paris Cedex 07.