JACQUET METALS ETHICS ALERT LINE USER GUIDE

Last update: May 2023

JACQUET METALS and its subsidiaries (the "Group") have set up a professional whistleblowing system (the "Alert Line") in compliance with French and European regulations.

This system is not designed to replace other whistleblowing systems established in the Company in accordance with applicable regulations, including reporting lines.

1. Scope of application

The Alert Line is available to all persons, including employees and third parties. It is designed to allow anyone to report facts or suspicions relating to:

- corruption, or any situation in breach of the Group Anti-Corruption Policy (the "Policy");
- fraudulent behavior;
- any behavior in breach of ethical principles or applicable legislation.

The Policy may be consulted via the Group intranet site and on the JACQUET METALS website. If you have any queries regarding the application of the Policy, please contact the Compliance Committee at: compliance@jacquetmetals.com.

2. Exercising the whistleblowing right

If an employee, manager or third party becomes aware of suspected behavior or circumstances falling within the scope of application of the Alert Line, he or she may exercise this right.

Suspected behavior or circumstances may be reported:

- via the Alert Line, which may be accessed on the Group website under the "**Compliance**" section at: https://www.jacquetmetals.com/index.php/en/ethics-compliance/;
- by contacting your **line manager**;
- by **sending a letter** to the Compliance Committee at the following address: Comité Conformité, JACQUET METALS, 44 Quai Charles de Gaulle, 69006 Lyon, France.

Messages sent via the Alert Line are received by the Chief Financial Officer, the Chief Legal Officer and the Internal Audit Director (together, the "Recipient").

The whistleblower **may decide to remain anonymous.** He or she may also use an email address that contains no surname or first name, thereby guaranteeing the whistleblower's anonymity.

The message must include a precise description of the reported facts to enable the Recipient to examine the admissibility of the disclosure and, where applicable, launch an investigation. It is strongly recommended that you attach any documents that might help to corroborate your disclosure.

If the whistleblower chooses to remain anonymous, the Recipient will be unable to contact him or her to obtain additional information. In such cases, therefore, the message must be as detailed as possible, failing which the disclosure may be dismissed due to lack of information.

If the whistleblower provides his or her contact details, he or she may be contacted by the Recipient during the admissibility review and/or investigation.

Whistleblower status provides general protection against any discriminatory measures, provided the whistleblower fulfills all of the following conditions:

- personally became aware of the facts reported (excluding cases of suspicion and knowledge via a third party);
- is acting in good faith (however, reported practices need not be factually proven: suspicions may be reported);
- is acting in a disinterested manner;
- is acting in a professional context.

3. Handling of disclosures

All disclosures made via any system must set out detailed facts, preferably supported by documents whenever possible. To enable the disclosure to be reviewed and investigated, the following information must be provided if possible:

- Description of the facts,
- Date of alleged facts,
- Persons implicated (full name, position),
- Group company involved,
- Supporting documents.

Disclosures submitted via the Alert Line are forwarded by email to the Recipient and the whistleblower receives automatic notification of dispatch. After this automatic notification is sent, the Recipient has seven days to confirm receipt of the disclosure if it has not been sent anonymously.

The Recipient examines the admissibility of the disclosure. During this stage, the Recipient may contact the whistleblower to obtain additional information or documents. At the end of this initial review, the Recipient may decide whether or not to open an investigation.
Depending on the results of the investigation, the Recipient shall decide on the corrective measures to be implemented, sanctions to be applied and the information to be communicated.

Where the disclosure is not anonymous, the Recipient shall notify the whistleblower, within three months following confirmation of receipt, regardless of how far the review has advanced, of the state of progress of the review and the steps contemplated or taken to assess the truth of the allegations.

4. Confidentiality

The Alert Line guarantees confidentiality and protection of the rights of each individual during the handling of the procedure.

The identity of the whistleblower and person(s) implicated shall be kept confidential. The Recipient and the persons responsible for collecting and handling disclosures are also required to observe confidentiality.

If the whistleblower chooses to remain anonymous, anonymity is guaranteed by:

- no recording of the relevant forms on the website,
- the website cookie policy.

The identity of whistleblowers and persons implicated and the information collected by the Recipient are treated with the utmost confidentiality and may only be disclosed to persons responsible for investigating the reported facts.

Sanctions are liable to be imposed for breaches of confidentiality.

5. Data storage

Where no action is taken further to a disclosure (submitted via the whistleblowing system), the personal data collected shall be destroyed or anonymized within two months after the review is closed. Disclosures submitted outside the system shall be destroyed without delay or anonymized.

When disciplinary or litigation proceedings are instituted against the person implicated or the person responsible for submitting an abusive disclosure, the data collected shall be stored until the end of the proceedings or until the end of the limitation period for appeals against the decision.

Data collected may be stored to ensure protection of the whistleblower or to allow tracking of ongoing infringements. Such storage shall be strictly limited to the two aforementioned purposes.