Effective from 17/12/2023

Information policy for the management of whistleblower reports for the Company Ocrim S.p.a.

Table of Contents

Foreword

Ocrim S.p.a., hereinafter referred to as the "Company", undertakes to guarantee protection against any form of retaliation to all collaborators and to all persons who, operating within the company's structure, should encounter and report any irregularity. We invite the reporting persons to use the Company's internal reporting channel to facilitate the resolution of problems encountered. The Company is committed to ensuring that reported violations are treated discreetly and confidentially, guaranteeing maximum protection and providing appropriate feedback throughout the process. Of course, anyone can make use of the external reporting channels, as can Law Enforcement in the most serious cases.

1. Entry into force of the regulation and publicity

1.1. The policy will enter into force on 17-12-2023. With the entry into force of this policy, all provisions previously adopted in this matter, in whatever form communicated, shall be deemed repealed and replaced by the ones contained herein.

1.2. A copy of the regulation may be posted on the company notice board and/or made available on the company intranet and/or attached to the communication (possibly in other forms) formalising its adoption and contains instructions on how to use it at the Company.

2. Scope of the regulation

This process concerns persons reporting irregularities and offences at the company (whistleblowers). Whistleblowers are people who cooperate or have close relations with the company and who detect irregularities and report them.

Such persons may be: employees, candidates, temporary workers, external collaborators, contractors and subcontractors, external consultants and all those who could potentially be threatened with retaliation that harms their economic, labour, professional, reputational, etc. interests.

The protection provided by this policy is also guaranteed to persons who assist the reporting person in the reporting process (facilitators), to third parties who have links with the reporting person (colleagues or relatives) and who might suffer retaliation in the workplace.

For the purposes of the provisions laid down in (It.) Legislative Decree no. 24/2023 referred to as the "whistleblowing process".

3. What to report

The internal reporting channel is intended for reports arising from a suspicion of the reporting person with regard to actual or potential violations and/or irregularities that have occurred, are currently taking place, have occurred or are very likely to occur, and with regard to attempts to conceal such violations.

A violation/irregularity is any act or omission that is illegal and related to the company, or that defeats the object or purpose of the legislation, company policies, and/or internal regulations. A violation may include, but is not limited to, the following:

- bribery or corruption
- fraud, money laundering, theft or misuse of company assets or funds,
- undeclared or poorly managed conflicts of interest,
- anti-competitive conduct,
- insider trading or market abuse,
- violation of sanctions,
- financial irregularities,
- data privacy violations,
- gross negligence, bullying, unlawful discrimination, workplace or sexual harassment,
- gross waste of resources or mismanagement,
- unsafe working practices and other significant health or safety problems,
- modern slavery and human rights violations,
- significant damage to the environment,
- retaliation against an informer or other person protected under this policy,
- any other behaviour that is unethical, in violation of company policies or procedures, or illegal.

4. How to report

Authorised personnel (see below) are available to provide support or advice on the company's whistleblowing process.

4.1. Reporting channels

Reports can be submitted by the following means:

- electronically in Italian or English, through the application of the Company Trusty Ag. (owner of the platform) by opening the link: https://kruzer.trusty.report/;

Further information on Kruzer S.r.l. can be found at the portal: www.kruzer.it

It is desirable for the reporting person to use, in the first instance, the internal reporting channel set up by the Company; however, in certain cases, the whistleblower has the option of approaching the ANAC (Italian National Anti-Corruption Authority - www.anticorruzione.it) directly.

Other forms of external reporting envisaged may be public disclosure and/or reporting to the judicial or accounting authorities.

The conditions justifying external reporting to the ANAC are as follows:

the internal reporting channel set up is not active or does not comply with the regulations;

no feedback was received from an initial internal report;

it is considered that an internal report may not be effective or may lead to retaliation;

there is a well-founded reason to believe that the violation poses an clear or present danger to the public interest.

The conditions justifying public disclosure are as follows:

- there was no response, within the deadline, after one internal and one external report;
- there is a well-founded reason to believe that the breach poses a clear or present danger to the public interest;
- it is believed that the report, whether internal or external, may lead to retaliation or may not be effective (e.g. concealment or destruction of evidence) or alleged collusion between the infringer and the reporter is suspected.

5. Content and identity of the reporting person

A report should include as much detail as possible about who, what, where, when, how and why in relation to the reported violation, as well as any supporting evidence that refers to such violation. Any further information on how the company might best proceed to process the reported violation is welcome.

Whistleblowers must enter their identity in the procedure; anonymity will however be guaranteed through exclusively two-way communication with the person handling the reports.

The identity of the reporting persons, as well as any other information from which their identity may be directly or indirectly inferred, must not be disclosed to anyone outside the personnel who are authorised and competent to receive and follow up reports, without the explicit consent of the reporting persons. Notwithstanding the above provision, the Company is obliged to disclose the identity of the reporting person when required by law, informing the reporting person prior to such disclosure, unless such information would jeopardise the relevant investigation or judicial proceedings. Unauthorised attempts to identify a reporting person or a person concerned are not permitted and will be subject to disciplinary sanctions.

6. Who processes the reports and how

6.1. Authorised personnel

The Company's internal reporting channel is managed by: **Kruzer S.r.l.** who is authorised to receive and follow up reports (hereinafter referred to as authorised personnel).

Authorised personnel have direct, free and confidential access to the Company's Management and to specialised consultants to whom they report directly on the progress of the reporting system. Authorised personnel have direct and unrestricted access to the appropriate resources necessary to ensure the impartiality, integrity, and transparency of the reporting system and its processes.

At present, the following persons are authorised to collect and handle reports in the first instance: Mr Daniele Umberto Spano, CEO of Kruzer S.r.l. (first collection and contact with the reporting persons); Mr Marco Moncalvo, Proprietor of MM Consulenze S.a.s. di Moncalvo Marco & C. and Mr Damiano Cagna, Head of Personnel of Ocrim S.p.a. (persons involved in the continuation of the initial investigation activities).

6.2. Report processing

The processing of a report takes place in the following stages, depending on the content of the report and its nature:

received - the report was received by the Company;

initial triage - the content of the report is assessed for categorisation purposes, taking preliminary measures, prioritising and assigning further processing. If a report is found to be false, unfounded, or irrelevant to the process laid down in the legislation, a rejection response is communicated with the reasons for it;

processed - the report is being handled, the accuracy of the allegation is being assessed, an internal investigation or action to recover funds is underway;

under investigation - the allegation is under investigation;

closed - the processing of the report has been completed; either no action is deemed necessary in response to a report, the establishment of facts leads to the conclusion that no further investigation is warranted, the report is referred to another process to be dealt with, or the investigation has been completed (regardless of whether the violation is confirmed or not).

The Company aims to process reports in a timely manner. Circumstances such as the complexity of the reported violation, competing priorities and other compelling reasons may require an extended period for the completion of the report's processing.

The Company treats reports confidentially, impartially and without bias or prejudice towards the reporting person or any other person involved in or witness to the reported violation.

The persons concerned, i.e. the persons named in the complaints, enjoy the presumption of innocence. The respective reports can be communicated to them at the appropriate time. Any investigation must be conducted in a manner that preserves confidentiality to the extent possible and is appropriate to ensure that the persons concerned are not exposed to reputational damage (information is shared on a strict need-to-know basis).

7. Communication with the whistleblowers

After submitting a report, the reporting person will receive an acknowledgement of receipt no later than **seven days** after receipt of the report, regardless of the medium used.

Confirmation of receipt of the report, via the online platform, is provided in the reporting person's mailbox accessible on the same platform, using the access credentials provided to the reporting person at the end of the report submission process. These credentials are also provided to anonymous reporters.

Authorised personnel maintain communication with the reporting person and, where necessary, request further information or evidence and provide feedback to the reporting person. This communication takes place via the reporting person's mailbox on the platform, or via other communication channels agreed with the reporting person.

The personnel tasked with handling the reports are entitled to know the identity of the reporting person and, if the reporting person does not provide it, the report may be filed. In any case, the Company must inform the reporting person of the decision taken.

Initial feedback is provided to the reporting person within 3 months of the submission of the report, or 6 months if there are justified and substantiated reasons. The feedback includes information on the action planned or taken as follow-up and the reasons for such follow-up. Feedback may be limited to avoid compromising possible investigations or other legal proceedings, as well as due to legal restrictions on what can be communicated about follow-up and results. In this case and where possible, the reporting person will be informed of the reasons for the limited feedback.

The final outcome will in any case be communicated to the reporting person.

8. How the reporting persons are protected against retaliation

Retaliation is defined as any threatened, proposed or actual, direct or indirect act or omission that occurs in a work context, is motivated by internal or external reports or public disclosure, and causes or is likely to cause unjustified harm to the reporting person.

Below are some examples of retaliation:

- suspension, layoff, redundancy or equivalent measures;
- demotion or refusal of promotion;
- change of job and/or place of work, reduction in salary, change in working hours;
- denied training;
- a negative performance evaluation or a negative reference of the reporting person's work;
- imposition or administration of any disciplinary measure, reprimand or other sanction, including a fine;
- coercion, intimidation, harassment or ostracism, isolation;
- discrimination, disadvantageous or unfair treatment;
- disclosure of the reporting person's identity;
- failure to convert the temporary employment contract into an employment contract of indefinite duration, if the employee had legitimate expectations that he or she would be offered permanent employment;
- non-renewal or early termination of the fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or financial loss, including loss of business and income;
- blacklisting on the basis of a formal or informal industry agreement, which may result in the person being unable to find future work in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

The Company does not tolerate retaliation of any kind and takes preventive action to ensure that it does not take place.

Any form of retaliation, including threats, is prohibited and must be reported immediately. Such reports can be sent using the Company's internal reporting channel.

Anyone involved in retaliation could face serious internal and potentially external consequences under the applicable laws or regulations. If the Company identifies anyone involved in retaliation, these individuals will be subject to disciplinary action, which could include dismissal.

Action to deal with a violation or wrongdoing by the reporting person, unrelated to his or her role in the complaint, is not considered retaliation. The Company takes all reasonable measures to protect the reporting persons from retaliation.

If it is established that retaliation is occurring or has occurred, the Company must take reasonable steps to stop and deal with such conduct and support the reporting person by reversing the retaliation's negative effect. Some examples:

reinstate the reporting person in the same or equivalent position, with equal pay, responsibility, job position and reputation;

facilitate equal access to promotion, training, opportunities,

benefits and rights; withdraw the litigation; bring an action for compensation for damage.

Following the report, the authorised personnel carry out an assessment of the risk of retaliation against the reporting person. Depending on the likely sources of harm identified through the risk assessment, the authorised personnel identify and implement strategies and actions to prevent retaliation or contain identified retaliatory behaviour, such as:

- protecting the identity of the reporting person;
- sharing information on a strictly necessary basis;
- communicating regularly with the reporting person;
- providing emotional, financial, legal or reputational support throughout the process;
- encouraging and reassuring the reporting person about the importance of reporting the violation and taking measures to promote his or her well-being;
- modifying the workplace or reporting modalities;
- warning the interested parties or others that retaliatory behaviour or breaches of confidentiality may constitute a disciplinary offence.

Authorised personnel monitor risks at various stages of the process, e.g. when deciding to investigate, during the investigation, once the outcome of an investigation is known, and after the case is closed.

The protections provided by this policy apply to the reporting person even if the reported violation is unsubstantiated, if the reporting person had reasonable grounds to believe that the information about the reported violation was true at the time of reporting.

In addition, informers who have reported or publicly disclosed information about violations anonymously, but who are later identified and suffer retaliation, will be entitled to protection under this policy.

Anyone who knowingly makes false reports will be subject to disciplinary and/or other legal action, which may include dismissal or, when appropriate, a libel suit.

9. Retention of reports and case reports

If the reported violation is not substantiated by authorised personnel and the relevant data are not required by the Company for any further proceedings, the report and all information collected relating to the report and its processing will be permanently deleted within 6 months after the case is closed.

If the reported violation is proven, the report and all information collected in connection with the report and its processing will be retained for as long as necessary for the establishment, exercise, or defence of the respective legal claims.

In any case, all documentation concerning reported cases may not be kept for more than 5 years.

10. Update and revision

All users may propose reasoned additions to this Regulation when deemed necessary. The proposals will be examined by the Company's Management.

This regulation is subject to periodic revision, also depending on the introduction of new work and/or IT tools, technological developments, or changes in legislation.

The Management