

SEU Whistleblowing Policy

In compliance with the provisions of Directive (EU) 2019/1937 (the “EU Whistleblowing Directive”) - which provides for shared minimum standards aimed at ensuring a high level of protection for individuals who report violations of European Union law and policies (as well as national laws to the extent required at Member States level), the Sappi Group has adopted a reporting system which allows for the management of reports, including anonymous ones, submitted by persons that acquired information on a violation in a work-related context. This policy primarily applies to all employees of Sappi legal entities located in the EU (the “Sappi EU Entities”), but also to other persons as described below and it co-exists with the Group Whistleblowing policy, which continues to apply to all Sappi employees.

Why do we have a SEU Whistleblowing Policy besides our Group Whistleblowing Policy

Sappi has put in place and made available to employees of Sappi EU Entities specific channels to report violations in compliance with the EU Whistleblowing Directive. This policy has the following main objectives:

- **To explain** the different channels a Whistleblower may use to submit a report of violations, and how such reports are to be handled by the Sappi Group;
- **To promote** a work environment in which the Whistleblowers feel comfortable to report, in an impartial and objective way and in good faith, concerns about facts that they consider to be violations of the law or of good professional practices;
- **Facilitate** the disclosure of such facts to stop them and prevent them from happening again and, if necessary, to apply appropriate sanctions;
- **Protect** the Whistleblower, as well as persons related to the Whistleblower and “facilitators”, against any form of revenge or retaliation;
- **Guarantee** the confidentiality of the reports as well as the details of the Whistleblower and of the reported person;

- Allow the Sappi Group to **maintain** the **trust** of its collaborators and stakeholders, preventing or remedying any illegal behavior or misconduct reported to the extent reasonably possible.

Sappi’s commitment to ethical business practices is set out in the **Sappi Code of Ethics**.

Since in some EU jurisdictions certain rules in addition to those of the Whistleblowing Directive may be provided by local laws, this policy can be integrated with “local” addendums aimed at explaining to Whistle-blowers which additional rules may apply in their specific countries, if any. The **SEU Whistleblowing Policy** should be seen in addition to our **Group Whistleblowing Policy** which sets out the provisions which are relevant to all Sappi units and employees group-wide regarding the reporting of misconduct and which remains fully applicable. Employees of Sappi EU Entities shall refer to this SEU Whistleblowing-Policy when reporting matters covered herein (see below under section “What can be reported”). When reporting matters not covered in this policy, the Group Whistleblowing Policy will fully apply.

Who can submit reports under this policy?

SEU Whistleblowing Policy

The following persons can submit a report pursuant to this policy, to the extent (where applicable) they have a work-related relationship with any of the Sappi EU Entities:

- Current and former employees, whether working full-time or part-time, for an indefinite-term or fixed-term, including temporary staff, volunteers, apprentices and interns, whether paid or unpaid;
- External stakeholders such as customers, suppliers, agents, business partners or subcontractors, and their staff;
- Job applicants;
- Shareholders as well as the members of administrative, management or control bodies, including members without executive powers.

What can be reported?

The following matters can be reported through the reporting channels described in this policy:

- Violations of the Sappi Code of Ethics or group policies and procedures;
- Violations of European Union Law and policies, including in the following fields:
 - public procurement;
 - financial services, products and markets, and prevention of money laundering, terrorist financing and the financial interests of the EU;
 - product safety and compliance;
 - transport safety;
 - protection of the environment;
 - food and feed safety, animal health and welfare;
 - public health;
 - consumer protection;
 - protection of privacy and personal data, and security of network and information systems;
 - areas relating to the internal market of the EU, including breaches of state aid rules, competition laws and corporate tax;

- A criminal offense (e.g., corruption, fraud), as defined by local laws;
- A threat or harm to the public interest;
- Additional violations or breaches that may be relevant in accordance with the law of specific jurisdictions (e.g. violations of Organizational Models adopted by Italian entities pursuant to Leg. Decree 231/2001). Please refer to the addendum to this policy related to your country, if any.

The Whistleblower must become aware of the facts reported in a work-related context.

The reporting channels covered in this policy are not designed as a platform for raising routine issues or complaints of a personal nature including, by way of example, Human Resources related issues, such as remuneration, career development and other matters of a similar nature. The system should also not be used for urgent health, security or safety issues: these types of issues should be reported in accordance with applicable Sappi policies.

How to report a violation

Reports of violations under this policy can be made through the **Sappi Ethics Hotline**, which is available 24-hours a day, 365 days a year and can be approached through various channels which are accessible through the group-wide [Convercent Helpline Portal](#). The portal is also referenced in the Sappi Group Code of Ethics.

Any matter under the scope of this policy can be reported in any of the following ways:

- In written form through the portal: refer to [*Report an Incident*].
- In oral form by calling the Convercent Helpline: refer to [*Prefer to speak to someone?*]. For international calls a drop-down list is made available to choose the caller's location for the

SEU Whistleblowing Policy

international number assigned to their country [*Dialling internationally?*].

Phone calls will be answered by an independent third party vendor. The third party agent will ask a number of questions which will help to create a report focusing on the facts surrounding the raised concern.

The Whistleblower will be given a reference number that identifies the call should the caller wish to call back later to provide additional information or follow up on what has been done about the violation which was reported.

The Whistleblowers have the right to request a **personal meeting**, which will be organized within a reasonable period of time by the Designated Function (as defined below).

The reporting channels available ensure that Whistleblowers can report in their native language to avoid potential language barriers.

As explained on the Hotline platform, the Whistleblower can choose whether to remain anonymous or to reveal his name and information. Anonymity adds complexity to the handling of cases but Sappi respects such choice and will treat such cases to the best of its ability.

In addition to the above internal reporting channels, secure **external reporting channels** (e.g. set up by competent authorities or anti-corruption agencies per country) ensuring confidentiality are also available. Whistleblower who report via external channels shall benefit from the same protection provided to those who report internally. Internal reporting, however, is encouraged to help ensure that reported misconduct can be assessed and addressed in a timely manner by independent persons with corporate insight.

External channels should be utilized if internal reporting channels are not available or ineffective (e.g. when the Whistleblower does not receive any feedback on a report made through internal channels) or if the

Whistleblower has good reasons to believe that if he made a report through internal channels, there would be no follow-up or this could lead to retaliation.

As mentioned, each Member State has designated a competent authority to receive, give feedback and follow up on external reports of violations. Please visit the websites of the authority designated in your country to check what specific rules and reporting modalities apply locally.

A Whistleblower may **publicly disclose a violation** (e.g. via social media or by informing the media or the press) and benefit from the protection provided to those who report violations through internal or external channels, if he either:

- reported internally or externally but no timely action was taken, or
- had reasonable grounds to believe that the violation constituted an imminent or manifest danger for the public interest, or in the case of external reporting, this channel would be insufficient as there is a low prospect of the violation being effectively addressed, or that there would be a risk of retaliation due to particular circumstances of the case.

Whatever the channel used, reports must be well-founded and in good faith, therefore, based on precise and consistent elements that led the Whistleblower to reasonably trust that circumstances reported are true. Reports should indicate the reported person (i.e. the person to whom the violation object of the report is attributed) and contain all the documents and information available to support the circumstances reported.

Who is the local contact person and who will receive the report?

An independent and specifically trained person (the "Designated Function") is nominated as the first point of contact and recipient of the raised

SEU Whistleblowing Policy

concerns (e.g. Group Internal Audit). Where necessary, and depending on the type of violation reported, the report may also be received on a need-to-know basis by other impartial persons without conflict of interest.

In each case all the persons that will receive the report are under the obligation to handle it with the utmost confidentiality, which will extend to the identity of the Whistleblower and of the person to whom the reported conduct is attributed, as well as the information collected during the investigation phase. Non-compliance with this obligation may lead to legal sanctions.

In which timeframe do we have to react if one blows the whistle?

Upon receiving a report Sappi is obliged to send to the Whistleblower an acknowledgement of receipt within seven (7) days. Additionally, Sappi has to give feedback to the Whistleblower within a period of three (3) months after receipt of the report.

What happens after one blows the whistle?

Once a report of violation has been submitted and qualified as falling within the scope of this policy, an investigation will follow which will be handled in a confidential, objective and thorough process.

The Whistleblower may be contacted in order to provide clarifications and/or additions to the information and documents provided.

Also, the reported person to whom the violation is attributed will be contacted in order for such person to exercise the right of defense provided, however, this is not incompatible with the need to correctly verify the facts covered by the report and/or will not likely result in potential forms of retaliation against the Whistleblower.

Reports will be dismissed if they are deemed:

- ungrounded;

- outside the scope of this policy;
- unverified.

In this case, the Designated Function shall inform the Whistleblower of the conclusion of the procedure. If previously informed, also the reported person will be notified.

If the report is ungrounded and made with willful misconduct or gross negligence by the Whistleblower, the Designated Function shall inform the competent corporate disciplinary function for possible activation of a disciplinary procedure in compliance with applicable law.

If the report is deemed grounded, the Designated Function will:

- INFORM the Whistleblower of the outcome of the investigation. If previously informed, also the reported person will be notified;
- SEND a report to the responsible person or department (e.g. HR) as the competent disciplinary function for the adoption of the necessary measures, according to the applicable contract and/or disciplinary system in compliance with applicable law.

The records related to reports (including all the documents produced during the investigation phase) shall be stored securely in such a way to protect confidentiality and for no longer than it is necessary for the purpose of adequately managing the whole procedure. Note that the retention period may vary from country to country.

Data Protection Requirements (GDPR)

The protection of personal data in accordance with the General Data Protection Regulation (GDPR) is of utmost importance to ensure that Whistleblowers' personal data is handled securely and lawfully. Appropriate measures (both organisationally, and system-wise) are in

SEU Whistleblowing Policy

place to help ensure that unauthorised persons do not have access to this information. SEU has developed a sufficient strategy in handling and protecting the processing of personal data as well as to manage deviations in local retention periods.

Some of the key measures taken to protect personal data include:

Access to Whistleblowers' personal data is limited to only those who need it to carry out their duties ("Need to know Principle").

Personal data are stored securely using encryption and access controls to prevent unauthorised access or disclosure.

A secure Whistleblowing hotline that Whistleblower can use to report concerns anonymously.

If there is a breach of Whistleblowers' personal data, the company will investigate the breach, take steps to mitigate the risk and prevent it from happening again (refer SEU Data Breach Notification Policy).

Whistleblower protection

Retaliation is a typical concern for persons that want to report a violation, because authors of misconduct, as well as those who benefit from misconduct, may attempt to retaliate against or victimise a Whistleblower, also in the attempt to protect themselves from legal or disciplinary action.

Should a Whistleblower have a concern regarding retaliation, that person is allowed to make his report using the confidential or anonymous reporting mechanisms provided for. Whistleblower should also ensure that no one else knows that they have made the report.

Sappi gives the assurance that we will not tolerate retaliation against any person who makes a report in good faith. Any form of retaliation or victimisation is itself a violation of company policy and possibly the law and can

be reported through the reporting channels described above.

Sappi gives assurance that we will not retaliate against, or disadvantage anyone who has made a report in good faith and that appropriate measures and sanctions will apply to anyone who retaliates against or disadvantages in any way good faith Whistleblower.

The protection of good faith Whistleblower also extends to:

1. Family members such as spouses, partners, parents, children, siblings, and other individuals who are financially dependent on the Whistleblower.
2. Co-workers and colleagues of the Whistleblower who may face retaliation as a result of their association or support for the Whistleblower.
3. Individuals who support the Whistleblower in connection with the good faith report of violation (facilitators).
4. Legal entities that the Whistleblower owns, works for or is otherwise connected with in a work-related context:

As already mentioned above, the protection does not apply to whoever knowingly and deliberately makes a false report, provides false statements, discloses misleading information, or in general acts in bad faith (for example through a defamatory or slanderous denunciation). These persons may incur sanctions and could be subject to legal actions in accordance with applicable laws.

Sappi adopted a Group Anti Retaliation Policy that we encourage all employees and stakeholders to become familiar with. Note that in relation to reports of violations submitted pursuant to this SEU Whistleblowing policy the protection against retaliation conduct provided

SEU Whistleblowing Policy

in the Group Anti Retaliation Policy extends to the persons/legal entities mentioned above.

policy