

Compliance channel - FAQs

What is a compliance channel?

An compliance channel offers an individual the chance to report something that may not comply with the law, organisational values and/or the code of ethics and conduct and which could seriously affect an organisation's operations and reputation.

You should make a report whenever you have a concern based on serious and credible grounds, and where the matter could negatively affect company.

You can also report a social concern whenever you identify real or potential adverse impacts on human rights.

Why report it?

Whistleblowing is important to promote high ethical standards and thus maintain trust of stakeholders in the organisation and its operations.

By reporting, you can help prevent the escalation of misconduct, accelerate the detection of improper practices or violations, and minimise potential harm to company and its employees.

How is my anonymity guaranteed?

The compliance platform is provided by an external partner - WhistleB. This partner is an independent service provider that establishes anonymous communication between the whistleblower/complainant and the people who receive the reports.

The compliance platform or channel is separate from the company IT environment.

The compliance platform does not track IP addresses or other data that could identify the individual making the report.

Reports can only be decrypted by designated people.

Nevertheless, we recommend that you use the communication channel from a device that is not connected to the company intranet: you can do so via your mobile phone or from your home, safely!

You can, if you wish, disclose your identity in the report, the whole process will be confidential and all the people involved in the investigation that will result from the report are bound by a duty of confidentiality.

What information should the report include?

To allow for a thorough investigation, the report must include a detailed description, including what happened, as well as when and where it occurred. You do not need to have concrete evidence of your suspicions, however, any report must be made in good faith and be based on the truthfulness of its content. You can submit text files and images through the compliance channel. All metadata from uploaded files is removed to ensure the anonymity of the whistleblower/complainant.

What happens after you submit a report?

After submitting a report, you will receive an ID and password.

The recipients of the report may send a response or a follow-up question, which should be referred to, using the ID and Password initially generated. It is very important that you keep your ID and password in a safe place – the only way to access communications of the compliance channel.

This dialogue, during which you may remain anonymous for as long as you wish, ensures that you can contribute effectively to a successful investigation process carried out by the investigation team.

How do I send a report?

You can send your report via the compliance channel, available [here](#). The web channel is device-independent and is available for smartphones, tablets, and PCs.

How to trust the secure management of information?

The Information Security Management System of the platform and the partner WhistleB is in compliance with ISO 27001, the latest international standard for information security. The compliance channel is set up to ensure that information security, including the management of personal data, is considered in all decisions during development and throughout its lifecycle. We guarantee the confidentiality, integrity and availability of data.

Is the report encrypted?

Yes, data is encrypted during transmission and storage.

Only authorised users can access the report. The partner

WhistleB cannot decrypt and read messages.

What is the role of the WhistleB partner?

WhistleB is an independent whistleblowing service provider contracted by company to provide a secure and reliable whistleblowing service. The WhistleB service enables anonymous communication between the whistleblower/complainant and the whistleblowing team.

How to proceed if case of loss of ID or password?

If the ID or Password is lost, cannot be recovered for security reasons. You can send a new report and refer to the original report.

If I report this, am I protected?

All whistleblowers/Complainants who, in good faith, make a complaint with serious grounds to believe that the information disclosed is true, and who have chosen the appropriate channel to make the complaint, are protected.

Reports made in bad faith, or lacking any basis of truth, may be internally sanctioned through the initiation of disciplinary proceedings which could result, depending on the seriousness of the alleged facts and proven bad faith, in dismissal without right to compensation or damages.

The protection conferred by law extends to people who assist the whistleblower/complainant in the reporting process, to third parties connected to the whistleblower/complainant, such as colleagues or family members who may be targets of retaliation, and to legal entities (or equivalent entities) for which the whistleblower/complainant works or has a professional link.

Acts of retaliation against whistleblowers/complainants are prohibited and legally and internally sanctioned. If you believe you are experiencing retaliation motivated by a report you made, please report this fact through the compliance channel, so that we can resolve the situation as swiftly as possible.

Retaliatory acts are presumed to be those acts and omissions that, directly or indirectly, occurring in a professional context and motivated by an internal report, cause or may cause, in an unjustified manner, material or non-material harm to the whistleblower/complainant. The law also provides for support measures for whistleblowers/complainants, such as legal protection, witness protection measures and certification as a whistleblower/complainant.