



Whistleblowing Policy

April 1st, 2023

Part I: Policy Statement

Interroll¹ is guided by the principles of sustainability. In order to meet our responsibility towards future generations, we ensure that our products and business processes are sustainable in ecological, economic and social terms and are always state of the art.

Our strategies and activities are guided by universal principles in the areas of human rights, labor standards, environmental protection and anti-corruption. We also strive to advance social objectives.

Interroll expects all its employees, including temporary and external staff and all other individuals (e.g. customers, suppliers, etc.) to comply with these principles. They are in line with Interroll's corporate values and are detailed in the Code of Conduct and in the Supplier Code of Conduct.

Interroll encourages employees, customers, suppliers, partners, shareholders and, more generally, the stakeholders of the Group to promptly report any conduct, which they reasonably believe violates applicable laws, regulations, internal control principles, company directives, instructions and rules, such as the Code of Conduct, Supplier Code of Conduct, or any professional standard.

The principles of this Policy do not affect – and do not in any way limit – the obligations to submit reports to the competent judicial, supervisory or regulatory authorities in the countries where Interroll companies operate, or the obligations to submit reports to any control bodies established in the Group.

This Policy replaces the Whistleblowing Policy dated September 21, 2021, with immediate effect.

Interroll Holding AG, Sant'Antonino, April 1st, 2023

A black ink signature, appearing to read "Ingo Steinkrüger", written in a cursive style.

Ingo Steinkrüger
Chief Executive Officer

A blue ink signature, appearing to read "Heinz Hössli", written in a cursive style.

Heinz Hössli
Chief Financial Officer



¹ „Interroll“ includes all fully consolidated Interroll legal entities

Part II: Scope, Responsibilities and Definitions

1. GENERAL SCOPE

Interroll encourages employees, former employees, interns, candidates, customers, suppliers, partners, shareholders and, more generally, the stakeholders of the Interroll Group to promptly report any conduct, which they reasonably believe violates applicable laws, regulations, internal control principles, company directives, instructions and rules, such as the Code of Conduct, Supplier Code of Conduct, or any professional standard.

The Whistleblower Policy applies to concerns about, suspected or actual criminal conduct, unethical conduct or other misconduct including a (suspected) breach of law by or within Interroll, including but not limited to:

- Accounting, internal accounting controls or auditing matters
- Tax evasion concerns
- Money laundering or terrorist financing
- Export control or sanctions violations
- Market manipulation or Insider trading
- Confidentiality or privacy breaches
- Theft, Fraud, Bribery or Corruption
- Environmental crimes or damages
- Health and Safety concerns (including physical and mental wellbeing)
- Undesirable behaviors
- Violations of human rights
- Severe violations of the integrity of the whistleblower system
- Violations of any other laws, regulations or Interroll policies



Personal grievances, such as harassment or bullying, are not generally covered by this whistleblowing policy. A separate employee grievance procedure is established in each Interroll company. However, employees are encouraged to report personal grievances as part of this whistleblowing policy if the locally established procedures have failed or the employee fear retaliation and seeks protection under the scope of the whistleblowing mechanisms.

2. INTERROLL COMPLIANCE OFFICE (ICO)

Responsible for the whistleblowing policy, whistleblower protection and case investigation is the Interroll Compliance Office (Abb. ICO) which consists of the Director Corporate Sustainability & Compliance, who acts as Group Compliance Officer and the Head of Group Internal Audit.

The ICO defines, implements and further develops the whistleblowing framework for the Interroll Group under the supervision and guidance of the Group Chief Financial Officer.

In course of case investigations, the ICO will directly report to the Audit Committee of the Board of Directors and to the Chief Financial Officer.

The ICO presents summaries on a regular basis to the Audit Committee of the Board of Directors, the CEO and the CFO of the Group.



3. CONFIDENTIALITY

All reported cases, independently from the used reporting channel are considered strictly confidential. Only the members of the ICO are permitted to disclose the existence and details of the report to another internal or external party/individual if deemed necessary to manage the case.

All internal or external parties/individuals informed about the existence and details of the report are required to keep the obtained knowledge strictly confidential.

4. ANONYMITY

All whistleblowers have the protected right to remain anonymous. To guarantee, that the whistleblower remains anonymous during the entire process it is highly recommended to use the EQS Integrity Line as reporting channel. Nevertheless, if another reporting channel is used it is guaranteed by Interroll, that only the initial recipient of the report and the ICO for investigation purpose are aware of the identity of the whistleblower. At any stage of the investigation only the members of the ICO with explicit, written consent of the whistleblower are allowed to disclose the whistleblowers identity.

5. PUBLIC DISCLOSURE

Whistleblowers have the right to make reports public as a last resort if all other reporting channels fail to produce results. Examples of this are Internet platforms or social media, or communication to the media, public officials, civil society organizations, etc. This could be considered if the reporter has not received appropriate feedback from the ICO within the expected period of three to six months.

The right of public disclosure is not granted if the whistleblower disagrees with the conclusion provided by the ICO and Interroll reserves the right to take legal action in the course of unjustified public disclosure to protect its integrity and reputation.

Part III: Reports of misconduct

6. REPORT

The report must be as detailed and documented as possible, to provide useful and appropriate information to effectively verify the validity of the events reported. Where this information is known to the whistleblower, it is particularly important for the report to include:



- a detailed description of the events that occurred and how the whistleblower became aware of them;
- the date and place of the event;
- the names and job positions of the persons involved, or information that enables their identification;
- the names of any other parties who can attest to the actions set out in the report;
- reference to any documents that could confirm that the reported actions did occur;
- supporting documents as attachments.

If no documentation or evidence are submitted in the initial report, further information can be provided at a later point of the investigation.

7. REPORTING CHANNELS

Interroll's whistleblowing channels can be used to raise these concerns (also anonymously), without fear of retaliation. It alerts management to allegations of crimes or other suspected misconduct and helps ensure appropriate and adequate action is taken to address the situation. Interroll has established different reporting channels for whistleblowers to report misconducts:

7.1 DIGITAL PLATFORM

Interroll decided to establish a digital whistleblowing system using EQS (operator of the system, see www.eqs.com). Whistleblowers can submit their reports, including attachments through the integrity line from EQS. The EQS Integrity Line can be accessed from the Internet as well as the Intranet (SharePoint). The platform can be used also after the submission to communicate anonymously with the ICO and provide further attachments and information.

This reporting channel ensures with encrypted data transmitted via secure and independent servers, that the whistleblower can remain anonymous during the entire process.

It is recommended to always access the EQS Integrity Line from private networks and personal devices.

To access the EQS Integrity Line, click [here](#).





7.2 EMAIL

Cases can be provided (also anonymously) to following mail contact:

compliance[at]interroll[dot]com

This reporting channel can be used with anonymous mail addresses to ensure a certain degree of anonymity but it is not fully ensured that the whistleblower remains anonymous during the entire process.

This mail address shall only be used if the communication is not done through the EQS Integrity Line.

7.3 POSTAL SERVICE

Cases including evidence can be provided to the following contact address

STRICTLY CONFIDENTIAL

Interroll Holding GmbH
Group Compliance Officer
Paul-Zumbühl-Straße 10-30
74847 Obrigheim
Germany

or

STRICTLY CONFIDENTIAL

Interroll Holding GmbH
Head of Group Internal Audit
Höferhof 16
42929 Wermelskirchen
Germany

With this reporting channel the initial submission can take place completely anonymous but further communication between the whistleblower and the ICO might be not possible without disclosure of the identity.

7.4 IN PERSON

Cases can be reported in person to the below listed individuals but due to the in-person report anonymity is not guaranteed:

7.4.1 INTERROLL COMPLIANCE OFFICE

Cases can be reported directly to the Interroll Compliance Office, either the Group Compliance Officer or the Head of Group Internal Audit. After receiving the report, they will immediately initiate the investigation process.

It is recommended to make in-person reports only to the members of the Interroll Compliance Office

7.4.2 MANAGING DIRECTORS

Cases can be reported to the Managing Director of the effected Interroll company. The Managing Director will immediately forward the case to the Group Compliance Officer to initiate the investigation process.

7.4.3 COMPLIANCE COORDINATORS

Cases can be reported to the locally nominated Compliance Coordinators. The Compliance Coordinator will immediately forward the case to the Group Compliance Officer to initiate the investigation process.

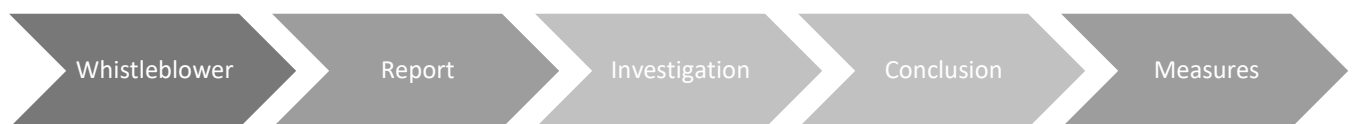
7.4.4 HUMAN RESOURCES

Cases can be reported to the Human Resource department of the effected Interroll company. The Human Resource department will immediately forward the case to the Group Compliance Officer to initiate the investigation process.

All cases – independent from the initial reporting channel – will be transferred for documentation purposes from the Group Compliance Officer to the EQS Integrity Line

Part IV: Investigation

8. INVESTIGATION PROCESS



1 | The whistleblower becomes aware of any (suspected) misconduct under the scope of this policy and collects evidence.

2 | The report is created and submitted through above defined reporting channel. If not reported through the EQS Integrity Line, the Group Compliance Officer will create a case within the Platform. All Documentation and written communication will be transferred to the EQS Integrity Line as well

3 | The ICO is responsible for checking the validity of the report on behalf of the entire Group, without prejudice to any specific local laws on the subject. As such it will perform a prompt and thorough investigation, in observance of the principles of impartiality, fairness and confidentiality towards all parties involved.

During the course of investigations, the ICO may request assistance from local Compliance Coordinators. Those local Compliance Coordinators are appointed by the Group Compliance Officer and they will for the course and matter of the investigation directly report to the ICO. Where appropriate, the ICO may also request the assistance of external parties (e.g. lawyers, forensic investigators, translators etc.) specializing in the area of the report,

provided their involvement is conducive to verifying the report and ensuring its confidentiality. The engagement of external parties in the case of investigation is excluded from the standard purchasing procedures and are under the sole decision making authority of the ICO after alignment with the Audit Committee and the Group CFO.

Often whistleblowers fail to provide all the necessary information in their initial report to allow their concern to be thoroughly investigated. Whistleblowers may also have additional evidence documents to facilitate the investigation or subsequent prosecution. It is therefore essential that the ICO is able to communicate with the whistleblower following the initial report. Through the EQS Integrity Line, this communication can be done anonymously and must be used if additional information for the investigation is required.

To gather information and evidence to further facilitate the investigation, the ICO will conduct interviews in person or using appropriate media like MS Teams meetings. By request and for the cause of the investigation the ICO will upon request receive access to systems, tools, and other file storage systems as well as all relevant data and information deemed relevant for the investigation. The required access is not limited to the Members of the ICO, also external parties involved by the ICO (e.g. investigators) receive system access where required. To ensure confidentiality, the access request is managed outside the standard procedures. After conclusion of the investigation provided access authorizations will be revoked.

4 | Once the investigation phase has been completed, the ICO will prepare a summary report on the investigations conducted and the evidence that they have considered.

Furthermore, it will report the results of the investigations and checks conducted for each report, to the company structures affected by its content.

However, if the investigations conclude that i) the existence of an offense can be clearly denied without conducting further investigative measures, ii) there is insufficient evidence or iii) that the events referred to in the report are unproven, the ICO will file the report together with the reasons why this action was taken.

5 | Based on the results, the ICO will then share the report with the company functions competent in each instance, so that they can draw up intervention plans and decide what measures must be implemented.

During the process of the investigation the Chief Executive Officer and Chief Financial Officer (if they are not subject to the investigation) will receive regular intermediate reports and updates of the investigation if of high relevance to Interroll.

Part V: Violations of the integrity of the whistleblowing system

9. WHISTLEBLOWER PROTECTION

Any kind of threat, retaliation, penalty or discrimination against the whistleblower or the reported party – or anyone who has participated in the investigation into the validity of the report – will not be tolerated.

No employee who raises genuinely held concerns in good faith using the whistleblowing mechanism described in this policy will be subject to any retaliation as a result of their action, even if their concerns turn out to be unfounded.

If whistleblowers believe that they are being placed at a disadvantage within the workplace as a result that they raised their concerns, they should immediately inform their Human Resource Department or the ICO.

Interroll reserves the right to take the appropriate actions against anyone who retaliates or threatens to retaliate against whistleblowers, who have submitted reports in accordance with this Policy.

10. BAD FAITH

It is understood that Interroll may take appropriate disciplinary and/or legal measures to protect its rights, assets and reputation against anyone who, in bad faith, has made false, unfounded or opportunistic reports and/or has made reports for the sole purpose of defaming, slandering, or causing damage to the reported party or to other parties mentioned in the report.

Part VI: Processing of personal data

The personal data of whistleblowers and of any other parties involved, e.g. the reported party/parties, that is obtained while handling the reports (including any sensitive data, such as racial and ethnic background, religious and philosophical beliefs, political opinions, membership in political parties or trade unions, and personal data indicative of a person's health and sexual orientation) will be processed in full compliance with the provisions of current legislation regarding the protection of personal data, and in any case in line with the provisions of the Group Directive Data Protection and their corresponding Instructions. Only the data strictly necessary for verifying the validity of the report and for managing it will be processed. The ICO, in their capacity as Data Controller (without prejudice to any specific local legislation on the subject) will process the personal data for the sole purpose of performing the procedures set out in this policy. Therefore, to ensure proper management of the reports received and to comply in full with legal or regulatory obligations, it will process the personal data with full respect for the privacy, rights, basic liberties and dignity of the persons involved.

Processing operations will be assigned to employees duly named as data processors, who will be supervised by the ICO and specifically trained to manage whistleblowing procedures, especially with regards to security measures and protecting the privacy of the parties involved and the confidentiality of the information in the reports.

The ICO may disclose the personal data of the reported party/parties contained in the reports to company boards and to the internal functions competent in each instance, as well as to the judicial authorities, in order to start the



procedures necessary for guaranteeing proper legal and/or disciplinary action against the reported party/parties, provided that the information collected and the checks carried out show that the contents of the report are true. In these cases, the personal data may also be disclosed to specialist external parties, as described in this policy. To avoid any misunderstanding, the personal data of the whistleblower remains confidential under all circumstances. All necessary measures will be taken to protect the data from accidental or unlawful destruction, loss or unauthorized disclosure during the activities to verify the validity of the report. Furthermore, the documents regarding the report shall be preserved in digital format on the EQS Integrity Line platform for a period no longer than necessary for the proper completion of the procedures established in this policy.