sqli

Internal whistleblowing procedure

Classification: C0 - Public

Version 1 – 02.07.2025

Preamble

SQLI is committed to full compliance with regulations and the highest standards of business Ethics and is firmly committed to upholding them in the conduct of its activities. This respect is not only a legal obligation, but also a fundamental pillar of our corporate culture, guaranteeing transparency, integrity and responsibility in all our professional interactions.

Ethics is a shared value and is everyone's responsibility. This responsibility is reflected both in employees' relations with each other and in their interactions with third parties. By adopting Ethicsal conduct, everyone contributes to creating a healthy and respectful working environment, where decisions are taken honestly and in accordance with our fundamental values. In this way, Ethics must guide our day-to-day behavior and our relations with stakeholders.

The internal whistleblowing system is in line with our Code of Conduct, which sets out the main principles and guidelines in terms of business Ethics for the SQLI Group, as well as the standards of behavior expected of all employees and corporate officers. This Code of Conduct is an essential reference for ensuring exemplary conduct within our organization.

In accordance with 2° of II of Article 17 of Law no. 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernization of economic life, known as "Sapin II", SQLI is required to implement "an internal alert system designed to enable the collection of reports from employees relating to the existence of conduct or situations contrary to the company's code of conduct".

This whistleblowing system must also take into account all applicable regulations.

In application of these various regulations, SQLI has chosen to set up a single internal alert system. This integrated approach enables more effective management of alerts and rigorous follow-up of reported cases.

The internal whistleblowing system described in this procedure replaces the previous system, improving it and meeting the Group's current needs and legal requirements. This change reflects our ongoing commitment to evolving and refining our practices, ensuring a safe working environment that complies with the strictest Ethicsal and regulatory standards.

Making a report in a nutshell:

What can be reported?

⇨ Any breach of national or international laws and regulations, any situation contrary to the SQLI code of conduct, and any infringement or risk of infringement of human rights, fundamental freedoms, safety, health or the environment.

How do I qualify for whistleblower status

⇨ Be a natural person acting in good faith and without financial consideration.

How do I report a problem

⇨ Using one of the three channels provided

1. **Secure email**: Send an email to Ethics.de@sqli.com , a secure mailbox accessible only to Ethics Officers, guaranteeing confidentiality of exchanges.
2. **Direct email**: Send an email to one of the Ethics Officers if the other is involved, using the Officer's business address with the words "Strictly Personal and Confidential - Internal Alert".
3. **Postal Mail:** Send a letter to SQLI - Ethics Officers SQLI Deutschland GmbH, Phönixseestr. 20, 44263 Dortmund - Germany **or** 2-10 rue Thierry Le Luron, 92300 Levallois-Perret, France mentioning "Strictly Personal and Confidential – Internal Alert" on the envelope. The letter can also be sent individually to (or to the Group Legal Counsel at the French address or the HR Manager at the German address)

The report will be received and processed by the Ethics Officers in accordance with the procedures described in this procedure.

Initial DR

I. General provisions

I.1 Purpose of the system

The purpose of this procedure is to set out the general principles of SQLI's internal whistleblowing system, and to explain how it works (who can report incidents? what can be reported? how to report? etc.)

The purpose of this procedure is also to recall the legal guarantees available to whistle-blowers, as well as the penalties incurred in the event of a breach of the applicable regulations

The System is always available on SharePoint LEGAL - Home .

I.2 Scope of application

The following people are eligible to use the Device:

- Any member of SQLI staff, whether permanent or temporary (including trainees), whatever their function, sector of activity or location, persons whose employment contract has ended, persons who have applied for a job with SQLI.
- SQLI shareholders and holders of voting rights
- Members of the administrative or management bodies of SQLI
- Any occasional external employee of SQLI
- Any third party, stakeholder of SQLI, and their subcontractors (members of their administrative, management or supervisory bodies and members of their staff): customer, service provider, supplier, partner, subcontractor, etc.
- Any employee or stakeholder of any entity of the SQLI group if the facts concern SQLI SAS.

I.3 Who are the people concerned?

To qualify for whistleblower status under the regulations, you must be a natural person acting in good faith and without consideration.

Good faith means that the person reporting must not deliberately make false accusations or have the sole intention of causing harm or gaining personal advantage. In other words, the whistleblower must act without malice or expectation of financial gain

Initial DR

The information disclosed by the whistleblower must have been obtained during his or her professional activity. Failing this, the whistleblower must have personal knowledge of the information

I.4 What can be reported?

The information that may be disclosed may relate to

1) A crime, a misdemeanor, a threat or harm to the general interest, a violation or an attempt to conceal i) a violation of an international commitment duly ratified or approved by Germany, ii) a unilateral act of an international organization taken based on such a commitment, iii) the law of the European Union, iv) a law or regulation
2) Any breach or conduct or situation contrary to SQLI's Code of Conduct
3) The existence or serious risk of harm to human rights, fundamental freedoms, human health and safety or the environment

These facts may relate to a variety of areas, such as corruption, fraud, influence peddling, anti-competitive practices, violation of rules and standards relating to international sanctions or embargoes, accounting, tax, financial or social irregularities, stock market irregularities, breaches of personal data protection, and so on

By way of example, the following facts may be reported under the Internal Alert System

- ⇨ In the economic and financial field
  - Tax fraud, insider trading, money laundering, embezzlement, accounts that do not reflect a true and fair view of the company
  - Obtaining or awarding a contract in return for financial advantage, collusion with a competitor, breach of the company's contractual commitments...
- ⇨ In the field of health, the environment, safety and personal protection
  - Discrimination, moral or physical harassment, forced labor
  - Serious breach of personal data protection: data leakage, use of data for non-legitimate purposes, etc.
  - Serious harm to health and safety
  - Serious damage

On the other hand, facts, information and documents, whatever their form or medium, the revelation or disclosure of which is prohibited by provisions relating to national defense secrecy, medical secrecy, the secrecy of judicial deliberations, the secrecy of judicial inquiries or investigations, or the professional secrecy of lawyers, are excluded from the Device

I.5 Confidentiality of the alert system

The present System guarantees the strictest confidentiality of the identity of those issuing the alert, of the persons concerned by the alert and of any third party mentioned in the alert. It also guarantees the strictest confidentiality of facts, information and documents communicated or collected while processing the alert

Initial DR

This reinforced confidentiality applies not only to all recipients of the alert, but also to any person, inside or outside the organization, involved in the investigation, processing and follow-up of the alert

People who use this System are assured that every precaution will be taken to guarantee that their identity and personal data will be kept strictly confidential. In this respect, the Referrers will take all necessary precautions to ensure that only the information required to carry out their mission is transmitted to the people who must intervene in the processing of the alert. Prior to any communication, these people will be made aware of the enhanced confidentiality inherent in the handling of an alert disclosed within the framework of the present System, and will sign a confidentiality undertaking

No information likely to identify the whistle-blower may be divulged without his or her consent, except for transmission to the judicial authorities when the persons responsible for collecting or processing the alerts are required to denounce the facts relating thereto. The whistle-blower is then informed, unless this information compromise the legal proceedings.

I.6 What guarantees are offered to the whistleblower / Absence of reprisals

⇨ Civil and criminal liability

- People who have reported or publicly disclosed information under the conditions provided by law are not civilly liable for damage caused by their reporting or public disclosure if they had reasonable grounds to believe, at the time they did so, that the reporting or public disclosure of all such information was necessary to safeguard the interests involved.
- These people are also exempt from criminal liability when they infringe a secret protected by law, provided that such disclosure is necessary and proportionate to safeguard the interests in question, that it is made in compliance with this procedure and with legal provisions, and that they meet the criteria for whistle-blowers as defined by this Procedure. They are not subject to any criminal sanction, in particular when they remove, misappropriate or conceal documents or any other medium containing the information of which they have been made aware in a lawful manner and which they report within the framework of the whistle-blowing procedure.

⇨ Prohibition of sanctions, discriminatory measures or reprisals:

No person may, by virtue of having reported an alert in compliance with the:

- Be excluded from a recruitment procedure or from access to an internship or period of professional training,
- Be sanctioned or dismissed,

Initial

- Be subject to any direct or indirect discriminatory measure, in particular with regard to remuneration, profit-sharing measures, distribution of shares, training, reclassification, assignment, classification, professional promotion, transfer or renewal of contract.
- Suspension, layoff or equivalent measure
- Demotion or refusal of promotion
- Transfer of duties, change of workplace, reduction in salary, change in working hours
- Suspension of training
- Negative performance appraisal or work certificate
- Disciplinary measures imposed or administered, reprimand or other sanction, including a financial penalty
- Coercion, intimidation, harassment or ostracism
- Discrimination, disadvantageous or unfair treatment
- Failure to convert a fixed-term or temporary contract into a permanent one
- Non-renewal or early termination of a fixed-term or temporary contract
- Damage, including damage to personal reputation (particularly on the Internet) or financial loss, including loss of business or income.
- Blacklisting
- Early termination or cancellation of a contract for goods or services
- Cancellation of a license or permit
- Improper referral for psychiatric or medical treatment

⇨ Provision of psychological and financial support measures: the competent authorities ensure the provision of such measures, including temporary financial assistance for whistleblowers, when they consider that their financial situation has seriously deteriorated as a result of the alert.

⇨ These same guarantees are offered to the following people:

- Facilitators: any natural or legal person under private, not-for-profit law who helps a whistleblower make a report.
- Individuals in contact with a whistleblower who are at risk of reprisals during their activities from their employer, their client or the recipient of their services.

II. Procedure

II.1 How to send an alert

Any whistleblower may choose to use the present internal whistleblowing system, which remains optional, or to make an external report or public disclosure, under the conditions set out below:

⇨ Internal whistleblowing: whistle-blowers may choose to alert their direct or indirect line manager, unless the latter is involved in the alleged facts, or the Ethics Officers as defined in article 2.2 below, in compliance with articles 2.3 and 2.4 of the present procedure.

Initial DR

- ⇨ External whistleblowing: whistle-blowers may also decide to send an external whistle-blowing report, either after having sent an internal report, or directly, to the following people:
  - To the competent authority designated by national laws
  - To the judicial authority
  - To an institution, body or agency of the European Union competent to collect information on violations falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019
  - To the Externe Meldestelle des Bundes beim Bundersamt für Justiz https://www.bundesjustizamt.de/DE/MeldestelledesBundes/MeldestelledesBundes_node.html

- ⇨ Public disclosure: Finally, public disclosure is possible in the following cases:
  - After making an internal or external report and taking no appropriate action in response, or
  - In the event of serious, imminent or obvious danger to the public interest, in particular where there is an emergency situation or a risk of irreversible harm, or
  - When referring the matter to a competent authority would expose the whistleblower to a risk of reprisals or would not enable the subject of the disclosure to be effectively remedied (risk of concealment or destruction of evidence, risk of conflict of interest or collusion).

II.2 Ethics Officers

SQLI's Ethics Officers are responsible for collecting alerts and reports made under this System, analyzing their admissibility, coordinating the investigation, drawing up an investigation report and keeping the whistleblower informed throughout the procedure

The Ethics Officers are also responsible for ensuring that the Code of Conduct is properly applied within the organization

Because of their position within SQLI, Ethics Officers have the skills, authority and resources required to carry out their mission. They receive regular training and are bound by a strict confidentiality agreement, which guarantees the impartiality required to carry out their mission

By decision of the General Management of SQLI, the Ethics Officers are, at the date of issue of the present procedure

- SQLI Deutschland HR Manager
- Group General Counsel

II.3 Referral procedures for Ethics Officers

Whistle-blowers can choose between the following methods of contacting the Ethics Officers:

Initial DR

- ⇨ **Send an email to** Ethics.de@sqli.com . This is a secure mailbox to which only the Ethic Officers have access, and who are the sole recipients of emails sent to it. All exchanges between the Ethics Officers and the whistle-blower will take place via this secure e-mail address and will be strictly confidential.

- ⇨ **Send an e-mail to one of the Ethic Officers only HR Manager Germany** if the other Ethic Officers is involved in the alleged facts. In this case, the whistleblower can send an email to the business address of the Ethics Officer he or she wishes to contact, specifying "Strictly Personal and Confidential - Internal Alert" in the subject line. The Ethic Officer concerned will then use his or her professional e-mail address to communicate with the whistle-blower, specifying "Strictly Personal and Confidential - Internal Alert" in the subject line of all communications.

- ⇨ **By post to** the **following address** SQLI – Ethic Officers – Phönixseestr. 20, 44263 Dortmund, Deutschland **or** 2-10, rue Thierry Le Luron - 92300 Levallois-Perret, France. The elements of the alert should be placed in an inner envelope, itself inserted in an outer envelope on which the words "Strictly Personal and Confidential - Internal Alert" should be written.

Alerts cannot be received orally.

II.4 Admissibility criteria / Alert content

To be processed, all alerts must:

- ✓ Written in German, French or English;

- ✓ Indicate the whistleblower's identity, contact details (professional or personal), position in the organization and/or link with SQLI.
  Anonymous alerts will not be processed unless they are of a particularly serious nature, which will be assessed by the Ethics Officers alone;

- ✓ Indicate the identity of the person concerned by the alert, his/her contact details (if known to the whistleblower), his/her position in the organization and/or his/her link with SQLI;

- ✓ Describe the facts that have occurred or are likely to occur, accurately and objectively;

- ✓ Be accompanied by any document, in any form or on any medium, to substantiate the facts and highlight their seriousness.

II.5 Checking and processing the alert

On receipt of an alert, the Ethics Officers send the whistle-blower an acknowledgement of receipt, by e-mail or by registered post with acknowledgement of receipt, within 7 working days of the date of receipt (either by e-mail or by post).

Initial DR

The Ethics Officers carry out a preliminary study of the admissibility of the alert received. They will check the following elements:

- Is the whistleblower authorized to issue a warning in accordance with article 1.2 of the present procedure?
- Does it meet the criteria defined in article 1.3 of the present procedure?
- Do the facts presented fall within the scope defined in article 1.4 of the present procedure?
- Do the documents supporting the content of the alert demonstrate the serious, objective and precise nature of the alert?

The Ethics Officers have a maximum of 30 days from receipt of the alert to declare it admissible or not, and to inform the whistle-blower accordingly. They may, before the end of this period, ask the whistle-blower to supplement his or her alert by providing additional information or documents in order to make the alert admissible.

If the alert is deemed inadmissible, the procedure ends.

If, on the other hand, it is deemed admissible, the Ethics Officers will take all necessary steps to deal with it. The alert may be investigated by the Ethics Officers, to establish or not the reality and materiality of the facts, while respecting the presumption of innocence.

To do this, the Ethics Officers can:

- Ask the whistleblower for further information, in writing, by telephone or by videoconference. In the latter two cases, if the whistle-blower consents in advance, the interview will be recorded. If the whistle-blower does not consent, the Ethics Officer will draw up minutes of the interview, which will be sent to the whistle-blower for verification, correction and approval. The finalized and validated minutes will then be signed by the Ethics Officer who conducted the interview and the whistle-blower.

- Request, if they consider it necessary, the intervention of one or more employees in view of their expertise or fields of intervention, unless they are the subject of the alert, or of third parties such as lawyers, experts or auditors. These people will be systematically made aware of the need for enhanced confidentiality in handling the alert and will sign a confidentiality undertaking. Only information and documents strictly necessary for their involvement in the investigation will be communicated to them.

Within 10 working days of the admissibility decision, the Ethics Officers inform the person concerned of the allegations, except where they consider that there is a risk of destroying evidence. Under no circumstances is the identity of the whistle-blower revealed to the person concerned by the alert.

Senior management may be informed of the most sensitive cases, except when it is implicated by the alert.

The Ethics Officers have 8 weeks from the date of receipt of the alert to investigate and draw up an investigation report.

II.6 Closing the alert

If the investigation report concludes that there has been no breach, or that the allegations are inaccurate or unfounded, the Ethics Officers close the alert and inform the issuer in writing.

If the investigation report concludes that a breach has occurred, or that the allegations are serious or well-founded, it is forwarded to General Management (except in cases where it is implicated in the facts concerned), which will take the appropriate decisions and the necessary corrective measures. These may include disciplinary action and/or legal proceedings against the employees involved.

The whistle-blower is informed in writing by the Ethics Officers, within a maximum of 3 months from receipt of the alert, of the corrective measures adopted and the closure of the alert.

II.7 Misuse and other penalties

Abusive and defamatory use of reporting channels may result in civil and/or criminal claims under applicable law.

III. Processing of personal data

III.1 Purpose and Data Controller

As part of the Internal Alert System, data is processed by SQLI, the data controller, to:

- Receive and process alerts or reports of a breach of a specific rule
- Carry out the necessary checks, investigations and analyses
- Define the action to be taken on a report
- Protect the people concerned
- Exercise or defend legal rights.

III.2 Legal basis

The processing carried out is carried out in order to fulfill the legal obligations incumbent on SQLI under Hinweisgeberschutzgesetz vom 31. Mai 2023 (BGBl. 2023 I Nr. 140), das durch Artikel 16 des Gesetzes vom 27. Dezember 2024 (BGBl. 2024 I Nr. 438) geändert worden ist.

III.3 Data concerned

As part of the Internal Alert System, the following data may be collected and processed:

- Whistleblower's identity, date and place of birth, ID number, e-mail address, duties and contact details
- Identity, functions and contact details of persons subject to the alert
- Identity, functions and contact details of people involved in the verification of reported facts and the associated investigation.
- Reported events that may involve sensitive data
- Information gathered during verifications and related investigations that may include sensitive data
- Interview and survey reports
- Alert follow-up

III.4 Data access and recipients

⇨ Internal transfer within SQLI :

- Personal data collected and processed as part of the Internal Alert System can be accessed and processed by the Ethics Officers;
- Necessary data can be passed on to employees not involved in the alert, who need to know in order to carry out verification actions;

Initial DR

- Data may also be forwarded to General Management, unless it is concerned by the alert, so that corrective action can be taken if necessary.

⇨ **Transmission to external service providers**: data may be transmitted to service providers (lawyers, experts, auditors, etc.) when they are called upon to intervene in the survey or for consultancy purposes. Only strictly necessary data will be transmitted.

⇨ **Transmission to third parties**: data may be transmitted to third parties in cases where SQLI is required to comply with applicable laws and regulations, as well as with legal requests and orders.

III.5 Shelf life

⇨ **When the alert is deemed inadmissible**: in this case, the data relating to the alert is archived after anonymization within two months of the date of inadmissibility. If it turns out that the alert was reported in bad faith or in an abusive manner, the data may be retained under the conditions set out below when disciplinary or legal proceedings are initiated.

⇨ **When the alert is deemed admissible:**

- And if it is not followed by disciplinary or legal proceedings: the data relating to the alert is archived after anonymization within two months of the date of closure of the alert;
- And if the alert is followed by disciplinary or legal proceedings: data relating to the alert is kept until the end of the proceedings or the time limit for appeals against the decision.

III.6 Security measures and transfers outside the EEA

SQLI implements the physical, organizational and technical security measures necessary to prevent any unauthorized access, disclosure, modification or destruction.

These measures include :

- Data storage on secure servers within the European Union
- Access limited to authorized persons with a need-to-know
- The implementation of internal organizational measures, such as the signing of confidentiality agreements where necessary.

Alerts issued from a third country outside the EEA may be processed in accordance with this procedure.

III.7 Rights of persons concerned

Any person identified in an alert has, in accordance with the GDPR and the DSGVO:

- a right of access to data concerning them, without however being able to invoke this right to obtain the identity of the whistle-blower.

Initial
DR

- a right to rectification and deletion of factual data that may be verified by SQLI, without this making it impossible to reconstruct the chronology of reported events or to delete or replace elements initially collected.

The right of opposition cannot be exercised by the people concerned, as SQLI is acting within the framework of its legal obligations.

All the above rights may be exercised at the following address: Ethics.de@sqli.com

DETCHEVERRY Renaud

Managing Director - SQLI International

Signed by:
DETCHEVERRY Renaud
EBF499896C674BB...