



SYNLAB

Third Party Speak-Up Policy

1. Scope of the Third-Party Speak-Up Policy

This Third-Party Speak-Up Policy ("**Policy**") is intended to encourage and enable business partners¹ and their respective employees as well as other third parties to report established or suspected breaches of the German Supply Chain Due Diligence Act (*Lieferkettensorgfaltspflichtengesetz*) and violations against SYNLAB's Supplier Code of Conduct ("**Reporters**").

2. General Principles

Notwithstanding the circumstances under which a report is made, SYNLAB adheres to and will apply the following principles to all situations and measures undertaken.

2.1. Protection of Reporters

SYNLAB believes that the functionality of third-party reporting on violations can only work following a transparent and trustworthy process in which Reporters are aware that they act in a safe and protected atmosphere. SYNLAB therefore commits to the following principles:

Non-retaliation: Reporters do not have to fear negative consequences of discriminatory or disciplinary nature for making a report in good faith or raising questions, doubts and concerns.

Fair trial: All cases will be subject to strict impartiality, the assumption of innocence applies and the right to be heard is granted.

SYNLAB furthermore undertakes all reasonable efforts to preserve the **confidentiality** of legitimate reporting and the information contained therein the widest extent possible. Therefore, reports can also be submitted anonymously².

SYNLAB however reserves the right to make disclosures if:

- Reporter has consented;
- Required for effectively investigating the report and taking related measures;
- Necessary for compliance with a mandatory legal obligations;
- Disclosure is mandatory under applicable law (e.g. law enforcement authorities).

2.2. Exception for Misuse

Intentionally misusing the reporting system under this Policy for abusive practice (i.e., filing reports in bad faith or as an act of revenge) is strictly prohibited. Reporters who use the reporting system in an abusive way are not protected by the principles set forth above and may face sanctions under labor-, criminal- and civil law.

Furthermore, we do not tolerate any kind of threats, detrimental behavior or acts of retaliation. Such conduct is itself a breach of our values and can result in disciplinary action.

2.3. Informing concerned Individuals

SYNLAB will reasonably inform the persons concerned by a reporting.

¹ A business partner of SYNLAB contracted for the supply of goods or the provision of services.

² Please note that investigations will be facilitated if reports are not made anonymously which allows follow up questions and clarifications.

Subject to the circumstances of the individual case SYNLAB may refrain from such information in order not to jeopardize the effectiveness of the investigation, the protection of evidence or the reporting process.

2.4. Data Protection

When handling reports, SYNLAB adheres to applicable data protection laws and data security standards.

Records of reports and the related investigation materials will be stored in accordance with applicable laws and to the extent this is necessary for the achievement of SYNLAB's legitimate interest, in particular the operation of the internal reporting channels and an effective compliance management. Other legitimate interests include the establishment, exercise or defense of legal claims or ensuring compliance with applicable statutory obligations to which SYNLAB is subject. Generally, three years after further storage is no longer legally required, records will be deleted in accordance with applicable data protection laws.

Unsubstantiated reports or information for other reasons regarded out of scope of this Policy will be deleted immediately in accordance with applicable laws and regulations.

3. Reporting Procedure and Case Management

The reporting procedure under this Policy is built to allow an efficient, secure and transparent handling of reports.

Reporters can support this ambition by providing information in a concise and sufficiently detailed manner, including supporting evidence where available.

3.1. Reporting and Follow-Up

Reports can be brought to SYNLAB via one of the following reporting channels:

Reporters can use SYNLAB's electronic whistleblowing tool via the following link: <https://synlab.integrityline.app>. This electronic reporting system is operated by EQS Group AG.

Reports can also be delivered directly via your point of reference at SYNLAB or SYNLAB's Chief Human Rights Officer.³

Confirmation of receipt of the report to the Reporter can be expected within seven (7) days and updates about its report status will be provided in accordance with applicable laws. People competent for the review of a report may reach out to the Reporter with follow-up questions and for clarifications.

3.2. Plausibility Check and Main Investigations

Through an initial **plausibility check** under the involvement of SYNLAB's competent functions, implausible cases will be eliminated and closed. The Reporter will be informed accordingly.

Cases found plausible will be subject to main investigations. Such in-depth assessment of the case will consider all available facts and is undertaken under involvement of the most suitable functions within SYNLAB (e.g., the departments of Human Resources, Compliance or Internal Audit), in accordance with

³ Please note that anonymity cannot be granted in these cases, inter alia for technical reasons.

the nature of the case. Potential conflicts of interest (e.g., of the accused or the investigating parties) are duly considered.

The assessment of the facts is undertaken without undue delay and within reasonable timeframe considering the factual circumstances of the case (e.g., severity, complexity, provided information and evidence etc.). External resources for the assessment may be involved on a case-by-case basis as required. SYNLAB will involve and cooperate with public authorities and other instances (works council, data protection officer (DPO) etc.) to the extent required under and in compliance with applicable laws.

As a result of the investigation, cases will be categorized and handled as follows:

- Reports on violations which cannot be proved will be closed as **unsubstantiated cases**. The closing decision is documented.
- Proven violations are rated as substantiated cases. These cases will be addressed with appropriate **remediation measures**.

3.3. Remediation measures

SYNLAB will decide on a case by case basis how to appropriately address substantiated cases in the most effective way, considering inter alia the following criteria:

- **Severity of the violation:** Assessment of degree of impairment (intensity or depth of an injury), and of number of people affected
- **Probability of the violation:** Probability that a risk will materialize in a violation
- **Urgency:** Pending risk or existing violation
- **Category of the violation:** Categorization of cases (e.g., criminal cases or offences) and circumstances (negligence, intent)
- **Reversibility of the violation:** Weighting of possibility of eliminating negative effects and required resources
- **Area of Violation:** SYNLAB's own business area or violations by a supplier

Potential remedial measures inter alia include:

- Business partner notifications, warnings, request for certifications or audits
- Exercise of commercial leverage to stop a violation
- Measures to factually reverse or compensate remains of a violation

Underlying remediation plans will be established by the concerned departments and are subject to approval by the Chief Human Rights Officer.

Remedial measures will be executed under supervision of competent SYNLAB functions as foreseen in the remediation plan.

3.4. Closure and documentation

After successful application of remediation measures and subject to confirmation by the Chief Human Rights Officer cases will be closed. The decisions of closing cases will be documented. In addition, the relevant SYNLAB functions will be informed about the closure of cases in order to derive the necessity for the adaptation or the adoption of new preventive measures.



3.5. Effectiveness Review

The effectiveness of this Policy and of remediation measures will be reviewed under the supervision of Chief Human Rights Officer on a regular basis and ad hoc as required. The Chief Human Rights Officer will provide SYNLAB's management with summary information on the status of proceedings under this Policy on a regular basis.