



SYNLAB

Política de denuncia de
irregularidades para terceros

1. Alcance de la política de denuncia de irregularidades para terceros

La presente política de denuncia de irregularidades para terceros (la "**Política**") ha sido elaborada para alentar y permitir a los socios comerciales¹ y sus empleados respectivos así como a terceros a denunciar presuntas y efectivas violaciones de la ley alemana de la debida diligencia en las cadenas de suministro (*Lieferkettensorgfaltspflichtengesetz*) al igual que violaciones del Código de conducta de proveedores de SYNLAB ("**Denunciantes**").

2. Principios generales

Sin perjuicio de las circunstancias bajo las que se comunica una denuncia, SYNLAB respeta y aplicará los siguientes principios a todas las situaciones y las medidas adoptadas.

2.1. Protección de Denunciantes

SYNLAB está convencida que las denuncias de violaciones por parte de terceros solo funcionarán eficazmente con arreglo a un proceso transparente y fidedigno en el que los Denunciantes aprecian que actúan en un ambiente seguro y protegido. Por lo tanto, SYNLAB se compromete a respetar los siguientes principios:

Falta de represalias: Los Denunciantes no deben tener miedo de consecuencias negativas de tipo discriminatorio o disciplinario por una denuncia comunicada de buena fe o por plantear preguntas, dudas y preocupaciones.

Juicio justo: Todos los casos estarán sujetos a una estricta imparcialidad. Rige la presunción de inocencia y se confiere el derecho a ser oído.

Por lo demás, SYNLAB se esforzará al máximo para conservar la **confidencialidad** de informes legítimos y de toda información que contiene en la medida de lo posible. Por lo tanto, los informes también pueden ser suministrados en forma anónima².

Sin embargo, SYNLAB se reserva el derecho a revelar información si:

- el denunciante ha dado su consentimiento;
- ello fuera necesario para investigar eficazmente el informe y adoptar medidas adecuadas;
- ello fuera necesario para cumplir obligaciones legales;
- la revelación es obligatoria conforme al derecho aplicable (p. ej. frente a autoridades policiales).

2.2. Excepción en caso de abuso

Está estrictamente prohibido hacer mal uso del sistema de informes con arreglo a esta directiva por fines abusivos (p. ej. presentar informes de mala fe o bien como venganza). Los Denunciantes que utilizan el sistema de informes en forma abusiva no están protegidos por los principios arriba indicados, pudiendo estar sujetos a sanciones según el derecho laboral, penal y civil.

Además, no toleramos ningún tipo de amenaza, comportamiento perjudicial o actos de represalia. Tal comportamiento será considerado como una violación de nuestros valores, pudiendo derivar en una acción disciplinaria.

¹ Un socio comercial de SYNLAB contratado para el suministro de mercancía y la prestación de servicios.

² Téngase en cuenta que será más fácil realizar investigaciones si los informes no se presentan en forma anónima, ya que en tal caso serán posibles preguntas complementarias y pedidos de aclaración.

2.3. Información de individuos afectados

SYNLAB informará de manera razonable a las personas afectadas por un informe.

Según cada vez las circunstancias de un caso individual, SYNLAB puede abstenerse de tal información para no perjudicar la eficacia de la investigación, la protección de las pruebas o el proceso de información.

2.4. Protección de datos

Al manejar informes y denuncias, SYNLAB observa la legislación de protección de datos aplicable y las normas de seguridad de datos.

Los registros de informes y los materiales de investigación relacionados serán almacenados con arreglo al derecho aplicable y en la medida en que fuera necesario para proteger el interés legítimo de SYNLAB, especialmente el uso de canales de informes internos y una gestión efectiva del cumplimiento. Otros intereses legítimos incluyen el reconocimiento, el ejercicio o la defensa de derechos legales o el cumplimiento de las obligaciones legales aplicables que rigen para SYNLAB. Por lo general, tres años después de que la ley ya no requiere un almacenamiento de los registros estos serán eliminados con arreglo al derecho aplicable de protección de datos.

Los informes infundados o denuncias consideradas por otros motivos como fuera del ámbito de esta directiva, serán borrados inmediatamente con arreglo a las leyes y la normativa aplicables.

3. Procedimiento de comunicación y manejo de casos

El procedimiento de comunicación con arreglo a esta directiva ha sido concebido para permitir un manejo eficiente, seguro y transparente de informes.

Los Denunciantes pueden contribuir a ello facilitando su información de manera concisa y suficientemente detallada, lo que incluye pruebas materiales si estuvieran disponibles.

3.1. Información y seguimiento

Los informes pueden ser comunicados a SYNLAB a través de uno de los siguientes canales de información:

Los informantes anónimos utilizan el proveedor para informes externos³, disponible en muchos idiomas a través de los contactos indicados en el anexo.

Los informes y las denuncias asimismo pueden ser enviados directamente a través de su punto de referencia en SYNLAB o por el oficial superior de derechos humanos (Chief Human Rights Officer) de SYNLAB.⁴

La confirmación de la recepción para el informante llegará dentro de siete (7) días y las actualizaciones sobre el estado de su informe serán facilitadas con arreglo al derecho aplicable. Las personas

³ La dirección e-mail y los teléfonos regionales son operados por el bufete jurídico Hogan Lovells International LLP.

⁴ Téngase en cuenta que en tales casos no será posible otorgar anonimato, entre otras cosas por motivos técnicos.

competentes para la revisión de un informe tal vez contactarán al informante con preguntas de seguimiento y para aclaraciones.

3.2. Prueba de plausibilidad e investigaciones principales

Por medio de una **prueba** inicial de **plausibilidad** con intervención de las funciones competentes de SYNLAB, los casos poco plausibles serán eliminados y cerrados. El informante será informado correspondientemente.

Los casos considerados como plausibles serán sometidos a investigaciones principales. Tal valoración profunda de un caso tendrá en cuenta todos los hechos y datos disponibles y se realizará con participación de las funciones más adecuadas dentro de SYNLAB (p. ej. los departamentos de Recursos Humanos, Compliance o Auditoría Interna) conforme a la naturaleza del caso. Se consideran debidamente posibles conflictos de intereses (p. ej. de la persona acusada o de las partes que realizan la investigación).

La valoración de los hechos y datos se realiza sin demora indebida y dentro de un marco de tiempo razonable considerando las circunstancias fácticas del caso (p. ej. gravedad, complejidad, información y pruebas aportadas, etc.). Según sea necesario podrá recurrirse a recursos externos para la valoración en casos individuales. SYNLAB contactará a y cooperará con autoridades públicas y otras entidades (comités de empresa, el responsable de protección de datos (DPO), etc.) en la medida necesaria y con arreglo al derecho aplicable.

Como resultado de la investigación, los casos respectivos serán calificados y manejados como sigue:

- Los informes sobre violaciones que no podrán ser comprobadas serán cerrados como **casos infundados**. La decisión sobre el cierre es documentada.
- Las violaciones comprobadas son calificadas como casos fundados. Estos casos serán abordados con **medidas de remediación** adecuadas.

3.3. Medidas de remediación

SYNLAB decidirá en cada caso individual cómo tratará adecuadamente casos fundados tan eficazmente como fuera posible, teniendo en cuenta los siguientes criterios:

- **Gravedad de la violación:** valoración del grado del daño (intensidad o profundidad de una herida y número de las personas afectadas)
- **Probabilidad de la violación:** probabilidad de que un riesgo se materializa en una violación
- **Urgencia:** riesgo pendiente o violación existente
- **Categoría de la violación:** calificación de los casos (p.ej. causas penales o infracciones) y de las circunstancias (descuido, dolo)
- **Reversibilidad de la violación:** ponderación de la posibilidad de eliminar efectos negativos y recursos requeridos para ello
- **Área de la violación:** área propia de negocios de SYNLAB o violaciones por parte de un proveedor

Las posibles medidas de remediación incluyen, entre otras cosas:

- notificación de socios comerciales, advertencias, pedidos de certificaciones o auditorías
- ejercer influencia comercial para detener una violación

- medidas para anular objetivamente una violación o bien para compensar los efectos de una violación

Los departamentos afectados elaborarán planes correctivos subyacentes que deben ser aprobados por el oficial superior de derechos humanos (*Chief Human Rights Officer*).

Las medidas de remediación serán llevadas a cabo bajo la supervisión de las funciones competentes de SYNLAB tal como está previsto en el plan de remediación.

3.4. Cierre y documentación

Después de la aplicación exitosa de las medidas de remediación y de una confirmación por parte del oficial superior de derechos humanos, los casos serán cerrados. Las decisiones sobre el cierre de casos serán documentadas. Además, las funciones relevantes de SYNLAB serán informadas sobre el cierre de casos a fin de derivar la necesidad para la adaptación o la adopción de nuevas medidas preventivas.

3.5. Revisión de la eficacia

La eficacia de esta Política y de las medidas de remediación será revisada bajo supervisión del oficial superior de derechos humanos (CHRO) tanto periódicamente como también ad hoc según fuera necesario. El oficial superior de derechos humanos facilitará regularmente a la gerencia de SYNLAB información resumida sobre el estado del procedimiento dentro del marco de la presente Política.

Anexo – Contactos para informes externos

Informes por **correo electrónico**: SYNLAB-Compliance@hoganlovells.com

Informes por **teléfono**:

País	Número de teléfono
Austria (alemán/inglés)	+49 8929012812
Bielorrusia (ruso/bielorruso/inglés)	+49 2111368800
Bélgica (francés/inglés)	+33 153672367
Brasil (portugués/inglés)	+55 0800 009 0016
Colombia (español/inglés)	+525 550910291
Croacia (croata/inglés)	+385 (0)1 2100 800
Ecuador (español/inglés)	+525 550910291
Francia (francés/inglés)	+33 153672367
Alemania (alemán/inglés)	+49 8929012812
Ghana (inglés)	+49 8929012812
Italia (italiano/inglés)	+39 02720252250
México (español/inglés)	+525 550910291
Nigeria (inglés)	+49 8929012812
Panamá (español/inglés)	+525 550910291
Perú (español/inglés)	+525 550910291
Polonia (polaco/inglés)	+48 225298650
España (español/inglés)	+34 91 349 8045
Emiratos Árabes unidos (árabe/inglés)	+971 4 3779 330
Reino Unido (inglés)	+49 8929012812



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.

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.



2.3. Informing concerned Individuals

SYNLAB will reasonably inform the persons concerned by a reporting.

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:

Anonymous Reporters use SYNLAB's external reporting provider³, which is available in many languages via the contacts provided in the Annex.

Reports can also be delivered directly via your point of reference at SYNLAB or SYNLAB's Chief Human Rights Officer.⁴

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 The email-address and the regional telephone numbers are operated by the law firm Hogan Lovells International LLP.

⁴ Please note that anonymity cannot be granted in these cases, inter alia for technical reasons.

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 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.

Annex – External reporting provider contact

Reporting via **Email**: SYNLAB-Compliance@hoganlovells.com

Reporting via **Telephone**:

Country	Telephone number
Austria (German/English)	+49 8929012812
Belarus (Russian/Belarussian/English)	+49 2111368800
Belgium (French/English)	+33 153672367
Brazil (Portuguese/English)	+55 0800 009 0016
Colombia (Spanish/English)	+525 550910291
Croatia (Croatian/English)	+385 (0)1 2100 800
Ecuador (Spanish/English)	+525 550910291
France (French/English)	+33 153672367
Germany (German/English)	+49 8929012812
Ghana (English)	+49 8929012812
Italy (Italian/English)	+39 02720252250
Mexico (Spanish/English)	+525 550910291
Nigeria (English)	+49 8929012812
Panama (Spanish/English)	+525 550910291
Peru (Spanish/English)	+525 550910291
Poland (Polish/English)	+48 225298650
Spain (Spanish/English)	+34 91 349 8045
United Arab Emirates (Arabic/English)	+971 4 3779 330
United Kingdom (English)	+49 8929012812