



www.synlab.com

CODE OF CONDUCT
SYNLAB LIMITED





Foreword

*Reliability and integrity have become key concepts in modern corporate governance. This is because sustained business growth is only possible when a firm is able to trust in the reliability of its shareholders, customers, suppliers and staff – locally and globally. Gaining such confidence can only be achieved by consistently upholding high standards of social and ethical conduct. This Code of Conduct (the "**Code of Conduct**") is intended to establish clear standards for all Synlab Members.*

Effective implementation of the Code of Conduct is a top priority for Synlab management, the Synlab Board of Directors and Synlab shareholders. This Code of Conduct is binding, with no exceptions. All Synlab Members are responsible for adhering to the Code of Conduct's provisions.

The Code of Conduct reflects our beliefs and values. It is an expression of our common understanding of integrity in our everyday course of business. The Code of Conduct outlines how these principles are implemented and applied in situations occurring in the daily course of business.

Every Synlab Member can contact his or her supervising manager, the responsible Regional Compliance Officer or a member of the Compliance Committee with questions concerning this Code of Conduct. The Board of Directors appoints the Chief Compliance Officer and the other members of the Compliance Committee. Potential violations either of laws, this Code of Conduct or any guidelines or procedures related to this Code of Conduct must be reported to the responsible Regional Compliance Officer, the Legal Compliance Officer or the Chief Compliance Officer. Reports may also be made to an independent Ombudsman in circumstances where one has been appointed. There will be no sanctions or reprisals as a result of reporting a breach or potential breach of this Code in good faith and in accordance with this Code of Conduct.

It is the personal responsibility of each and every one of us to strive to ensure that the Synlab Group will at all times retain its good reputation around the world, being seen as a business partner with ethics and integrity.

29 November 2016

*Dr. Bartl Wimmer
Chief Executive Officer and
Director*

*Vincent Marcel
Chief Financial Officer and
Chief Compliance Officer*



Important Defined Terms

The term "**Associated Companies**" refer to all entities that Synlab Limited can require either directly or indirectly to adopt this Code of Conduct by virtue of a majority voting interest, a majority in the entity management, agreement(s) and/or the constitutional documents of that entity and/ or which are consolidated in the financial statements of Synlab Limited.

The terms "**Synlab**", the "**Synlab Group**" and the "**Company**" refer to Synlab Limited and its Associated Companies.

The term "**Synlab Member**" or "**you**" refers to any Synlab Group director, officer, consultant or employee (either temporary or permanent), as well as to all staff practising on a contract basis (including based on a *convention d'exercice libéral*) within the Synlab Group. The use of these terms is not intended to confer a status of employment where one does not otherwise exist.



Content

1. FUNDAMENTAL RULES OF CONDUCT	1
1.1. LEGAL AND ETHICAL CONDUCT	1
1.2. RESPONSIBILITY FOR THE SYNLAB GROUP REPUTATION	1
1.3. MUTUAL RESPECT, HONESTY AND INTEGRITY	2
1.4. LEADERSHIP, RESPONSIBILITY AND SUPERVISION: SPECIAL MANAGEMENT DUTIES	2
1.5. IMPLEMENTATION AND MONITORING OF CODE OF CONDUCT COMPLIANCE	2
1.6. COMPLIANCE ORGANISATION	3
1.7. REPORTING	3
2. SOCIAL CONDUCT WITHIN THE COMPANY: INTERACTIONS WITH COLLEAGUES AND OTHER STAFF	5
2.1. FAIR AND EQUAL TREATMENT	5
2.2. PERSONAL DIGNITY	5
2.3. PUBLIC IMAGE	6
2.4. CONFLICTS OF INTEREST	6
3. DEALINGS WITH CUSTOMERS, PATIENTS, BUSINESS PARTNERS AND PUBLIC OFFICIALS	7
3.1. NO SPECIAL BENEFITS OR PERKS FOR CUSTOMERS OR CUSTOMER REPRESENTATIVES	7
3.2. LEGAL ANTI-CORRUPTION FRAMEWORK	8
3.3. SPECIAL RULES FOR DEALINGS WITH GOVERNMENT REPRESENTATIVES AND PUBLIC OFFICIALS	8
3.4. BRIBERY OF EMPLOYEES OF PRIVATE ENTERPRISES IS ILLEGAL	8
3.5. INVITATIONS AND GIFTS TO AND FROM PRIVATE-SECTOR CUSTOMERS	8
3.6. TREATMENT OF DISCOUNTS, COMMISSIONS AND CONSULTANT CONTRACTS	9
4. DEALING WITH SUPPLIERS AND EXTERNAL SERVICE PROVIDERS	11
4.1. GENERAL RULES FOR DEALINGS WITH SUPPLIERS AND EXTERNAL SERVICE PROVIDERS	11
4.2. PROVIDER DISCRIMINATION IS PROHIBITED	11
4.3. ACCEPTING BENEFITS FOR ONESELF OR A THIRD PARTY IS PROHIBITED	11
4.4. ACCEPTING INVITATIONS	11
5. COMPETITION AND ANTITRUST LAW REQUIREMENTS	12
6. BAN ON INVOLVEMENT IN MONEY LAUNDERING	13
7. ECONOMIC SANCTIONS	15
8. PROTECTING COMPANY ASSETS AND FINANCIAL INTEGRITY	16
8.1. ACCURATE AND COMPLETE DATA, DOCUMENTS AND REPORTING	16
8.2. SAFEGUARDING SYNLAB GROUP ASSETS	17
8.3. INTELLECTUAL PROPERTY AND THIRD-PARTY COPYRIGHTS	17
8.4. IT SYSTEMS USE AND SECURITY	17
9. DATA PROTECTION	18
10. OMBUDSMAN	19



1. Fundamental rules of conduct

The Code of Conduct is based on fundamental rules. These represent basic guidance for our actions, defining the essentials for adherence to laws and ethical standards, and also represent goals which all of us work towards fulfilling in the interests of the Synlab Group, Synlab Members and business partners. These basic conduct rules provide a reliable guide to proper action in case of doubt.

The Code of Conduct applies to Synlab Limited and all Associated Companies, as well as all Synlab Members.

Synlab expects its business partners to adopt high standards of conduct equivalent to those contained in this Code of Conduct. Consultants and other business partners may only be engaged by the Synlab Group after careful and diligent selection and in strict accordance with the Code of Conduct in order to avoid even the appearance of a violation. The Synlab Member who hires or commissions any consultant or provider is personally responsible for instructing those parties and monitoring their activities.

Non-compliance with the Code of Conduct or any guidelines¹ or procedures related to the Code of Conduct exposes Synlab Members and possibly the Company itself to civil liability claims and potential criminal prosecution. The Synlab Group thus demands a high degree of integrity and responsibility from every Synlab Member.

You must report any conflict between any provisions of this Code of Conduct (or any guidelines or procedures related to the Code of Conduct) and your contract of engagement with Synlab to your Regional Compliance Officer immediately.

1.1. Legal and ethical conduct

Compliance with applicable laws is the absolute cornerstone of the conduct of each Synlab Member. All Synlab Members comply with the law. In international business this means both the laws of your own country and those of any other countries concerned.

'Laws' in this context and in the context of this Code of Conduct means all applicable legal provisions.

Violations of laws are strictly prohibited. When a violation is discovered, the actions of the individual concerned are subject to thorough investigation regardless of the individual's position in the Synlab Group, and legal consequences will follow accordingly in view of the breach of duty, including termination of employment.

Outside the legal realm, we furthermore practise ethics. This fosters the level of trust and reliability, which is essential for running a major corporation. Compliance with rules of ethics is a fundamental obligation of every Synlab Member. All managers are thus to serve as role models.

1.2. Responsibility for the Synlab Group reputation

The reputation of the Synlab Group and our perception by the public and customers depend upon the conduct of each one of us. Inappropriate behaviour on the part of one single Synlab Member can have a serious negative impact on the Synlab Group. Every Synlab Member must be aware of his or her responsibility for the Company's reputation, and must act accordingly, particularly in the performance of his or her contractual duties.

¹ Please note that in certain countries in light of particular laws, country-specific guidelines may be necessary.



1.3. Mutual respect, honesty and integrity

The Synlab Group and Synlab Members respect personal dignity and the rights and diversity of the individual, both within and outside the Company. The Synlab Group and Synlab Members condemn any form of discrimination, harassment (including sexual) and insulting or aggressive behaviour. The Synlab Group and Synlab Members are open and honest, and fulfil their responsibilities as reliable partners, both internally and externally.

1.4. Leadership, responsibility and supervision: special management duties

Every manager is responsible for the Synlab Members reporting to him/her and also has duties towards all Synlab Members with whom he/she interacts. Managers are role models. Respect must be earned through impeccable personal behaviour, achievement, integrity and social competency (including behaviour free from harassment, insult and aggression), and every Synlab Member must adhere to these values. Managers are trusted by Synlab Members to set clear objectives which are ambitious but realistic. They promote career development, and are open to hearing the problems and concerns of their reports.

Every manager has organizational and supervisory responsibilities within their area of duty, and monitors compliance with laws, the Code of Conduct and any guidelines or procedures related to the Code of Conduct.

Managers select suitable Synlab Members based on their professional skills and personal competencies, taking into account the relative importance of the specific tasks involved and the Synlab Member's performance capability.

Synlab Members are to be given instructions, which are understandable, complete and binding.

Violations of laws, the Code of Conduct or any guidelines or procedures related to the Code of Conduct are not tolerated. Synlab Members should be informed of the potential consequences of a breach of duty. Any such violation must be systematically acted upon so as to uphold the interests of the Synlab Group. Reports of such violations are to be investigated carefully where merited.

1.5. Implementation and monitoring of Code of Conduct compliance

Compliance with the Code of Conduct is ensured through comprehensive acceptance of the principles above by all Synlab Members. Managers have particular responsibility as role models. All Synlab Members must be familiar with these rules of conduct, accept them and apply them as the basis for their actions if the Synlab Group is to remain an enterprise worthy of the recognition and reputation we have enjoyed for many years.

The Synlab Group is developing a training program for its managers who are, in turn, responsible for training the Synlab Members reporting to them. Training for specific functions (purchasing and procurement, as an example) is also developed.



1.6. Compliance Organisation

Our compliance function is organised as follows:

The Board of Directors appoints the **Chief Compliance Officer**, whose duties include:

- further development of the Synlab Group compliance system, including Synlab Member training;
- implementation of the compliance system in accordance with Group management specifications, in consultation with the Compliance Committee;
- processing of all compliance-related matters which are not the responsibility of the Compliance Committee; and
- regular reporting regarding compliance issues.

The Board of Directors also appoints the members of the **Compliance Committee**, upon recommendation from the Chief Compliance Officer. The Compliance Committee is chaired by the Chief Compliance Officer, who is also the Group Chief Financial Officer.

The Chief Compliance Officer appoints the **Regional Compliance Officers** for national and international Synlab locations. The list of the members of the Compliance Committee and the list of the Regional Compliance Officers is published from time to time by Global Marketing and Communications.

The Compliance Committee is to adopt terms of reference governing its operation and activities.

1.7. Reporting

All Synlab Members must provide information (verbal and written) concerning cases involving compliance issues (violations of laws, the Code of Conduct or any guidelines or procedures related to the Code of Conduct) to the responsible Regional Compliance Officer, the Compliance Legal Officer, the Chief Compliance Officer or the Ombudsman in circumstances where one has been appointed. **Tip-offs and reports are treated as confidential wherever possible in accordance with applicable law and may be given anonymously through the Chief Legal Officer or the Chief Compliance Officer or Ombudsman (where one has been appointed)** (see further information below).

Synlab Members who report concerns in good faith and in accordance with this Code of Conduct will not be subjected to detrimental treatment by the Company as a consequence of raising such concerns.

Upon receiving information regarding ongoing actions which they consider may potentially represent serious compliance violations posing a risk of substantial civil or criminal penalties for the Synlab Group and/or the Synlab Members, the respective Regional Compliance Officers are authorized to stop the activities in question and call for a decision by the responsible senior executive ("veto right").

The Regional Compliance Officer must report in writing such violations to the Compliance Committee. The Compliance Committee may take action to address the potential violation, and must report potential violations it considers significant to the Group Chief Executive Officer as soon as possible. The Group Chief Executive Officer, in turn, informs the Board of Directors where he considers that such information is warranted under the circumstances. The Compliance Committee must present an annual report to the Board of Directors setting out details of reports of violations, potential violations and compliance-related activity.



The Synlab Group may appoint an external attorney to act as Ombudsman for certain jurisdictions. Where one has been appointed, the Ombudsman's role is to receive confidential reports on potential violations of laws, the Code of Conduct or any guidelines or procedures related to the Code of Conduct, review these and forward information to the Compliance Committee as necessary. Section 10 of this Code of Conduct contains further details regarding the Ombudsman's responsibilities.

In case of doubt in assessing a particular situation, Synlab Members should always contact the Regional Compliance Officer responsible for their organizational unit, the Legal Compliance Officer or the Chief Compliance Officer especially if the answer to any of the following questions is 'YES':

- Is the activity illegal?
- Is the activity inconsistent with the Code of Conduct or any guidelines or procedures related to the Code of Conduct?
- Does the activity expose the Synlab Group to substantial economic, legal or reputational risk?
- Is the activity in violation of the Synlab Group obligations or commitments?
- Is there a gut feeling that something may not be right regarding the activity?

If the answer is 'YES' to one or more of the questions above, the Synlab Member must notify the Regional Compliance Officer, the Legal Compliance Officer or the Chief Compliance Officer, or the Ombudsman (where one has been appointed) about the activity or incident without delay.



2. Social conduct within the Company: Interactions with colleagues and other staff

2.1. Fair and equal treatment

We respect the rights and dignity of every individual Synlab Member. A corporate culture of fair treatment, mutual respect and trust in our human interactions forms the basis for successful cooperation between all Synlab Members.

We have the same esteem for all Synlab Members regardless of their nationality, cultural background, religion, ethnic origin, gender (and gender identity), disability, marital status, parental status, sexual orientation or age.

Every Synlab Member is entitled to fair and equal treatment, and a work environment free of discrimination or harassment.

Just as every manager has special responsibility, every Synlab Member must contribute as well to businesslike yet friendly and equitable dealings with other Synlab Members and outside parties in a spirit of partnership free of discrimination. This requires openness and tolerance in our mutual interactions, which the Synlab Group is dedicated to promoting.

Managers are required to work towards these goals as part of their responsibilities and to identify and immediately remedy any problem situations. Synlab Members are required to report violations and may seek advice regarding any related concerns pertaining to their own situation or that of another Synlab Member.

2.2. Personal dignity

Every Synlab Member has the right to be treated fairly and with courtesy and respect. The Synlab Group protects Synlab Members' personal dignity, and will not tolerate any form of abuse or harassment at work.

You must consider your own behaviour to ensure that you do not intimidate, offend or disparage others, and refrain from any conduct construable as moral or sexual harassment. Colleagues, co-workers and superiors must always be treated with respect and dignity. The following is not intended to be a comprehensive list but sets out examples of conduct to be avoided:

- failing to respect the religious convictions of others;
- misusing others' personal data
- spreading rumours; and
- communicating with a Synlab Member (including orally or in writing) in an insulting or aggressive manner.

Synlab Members who feel they are victims of discrimination or harassment may without any restrictions file a complaint with a Regional Compliance Officer, the Chief Compliance Officer or the Compliance Committee. The Regional Compliance Officer, the Chief Compliance Officer or the Compliance Committee will consider any complaint, review the matter carefully, investigate when appropriate and notify the Synlab Member filing the complaint of the review findings. Where appropriate the complaint may be passed to those responsible for human resources, who may take any action within their normal authority.



2.3. Public image

The Synlab Group supports Synlab Member involvement in public functions on a local and national level. Synlab Members must ensure that such involvement does not impair the Synlab Group's public image and is not contrary to the Synlab Anti-Corruption, Anti-Bribery and Sanctions Guidelines adopted pursuant to the Code of Conduct (the “**ABC and Sanctions Guidelines**”). When expressing personal opinions, one's connection with the Synlab Group should not be mentioned.

2.4. Conflicts of interest

A conflict of interest exists if the private interests of a Synlab Member could potentially undermine or impair Synlab Group interests.

Any activities and situations which could lead to a conflict between a Synlab Member's personal interests and the business interests of the Synlab Group, or which may have the appearance of such conflict, are to be avoided. Synlab Members must report any potential conflict of interest to their supervising manager or the Regional Compliance Officer.

The following are examples of situations which could lead to a conflict of interest:

- While working for Synlab you are employed by another company, especially if that company is a competitor or supplier of the Synlab Group (or could become a competitor or supplier in the foreseeable future);
- you have business relationships with a company in/at which a relative, spouse or other related party holds shares, is an employee or is a member of management;
- you have significant financial interests in a company or are involved in management of a company which is a Synlab Group supplier or customer; or
- you accept emoluments, gifts or favours in excess of the levels provided for by the **ABC and Sanctions Guidelines**.



3. Dealings with customers, patients, business partners and public officials

The Synlab Group bears responsibility towards patients and customers, which is why all Synlab Members must:

- respect patients' dignity and right to self-determination;
- respect patients' sphere of privacy;
- be sensitive to the patients' situation;
- conduct themselves properly even in the event of disagreement;
- pay due attention to what patients communicate, and
- respond objectively to criticism from patients.

In particular, Synlab Members who are medical staff must:

- practise their medical profession conscientiously, in accordance with principles of medical and human ethics, and in compliance with applicable laws and the conduct code of the medical professional;
- practise their medical profession responsibly and independently, accepting no instructions from non-physicians concerning diagnosis or treatment when practising in their primary field of medical expertise;
- respect patients' right to free choice of physician and to changing physicians; and
- consult with medical professionals unaffiliated with the Synlab Group for assistance with diagnosis or treatment, and respect patients' requests to get a second physician's opinion or be transferred to another physician's care.

The Synlab Group rejects and prohibits all forms of market influence, especially collusive arrangements affecting offers, prices and markets.

We compete for contracts by offering quality services and high-performing business locations. As set out further in the **ABC and Sanctions Guidelines**, Synlab Members are prohibited from directly or indirectly offering or providing customers or related parties any special benefits or perks in connection with Synlab activities.

For the purposes of this section 3, please also refer to the relevant provisions set out in the **ABC and Sanctions Guidelines**.

3.1. No special benefits or perks for customers or customer representatives

Offering, promising or giving benefits to Synlab Group customers or related parties in order to secure orders or otherwise illegally obtain opportunities or advantages for the Synlab Group is prohibited. It makes no difference whether the customer or customer representative is a public official, representative of a government entity or a person working in the private sector.

We reject all such practices, as these may impair fair competition or be in breach of anti-bribery laws, thus harming our business and the economic future of every Synlab Member.



3.2. Legal anti-corruption framework

The meaning of the word 'corruption' includes the illegal exchange of benefits (which for the purposes of the Code of Conduct should be taken to mean any advantage or value, irrespective of whether material or immaterial, which improves the situation of the recipient and which the recipient is not entitled to claim). Improperly influencing decisions or actions – anywhere in the world – by either offering, promising or granting benefits, or by accepting, agreeing to accept or soliciting benefits, may constitute bribery, which is a criminal offence in most countries. Both grantor and recipient of the benefit may be punished.

Corruption is a criminal offence which may lead to prosecution anywhere in the world.

3.3. Special rules for dealings with government representatives and public officials

It is a criminal offence in most countries to offer, promise or give anything of value to a public official in order to influence him/her in his/her official capacity. This is because there is great interest in protecting state organizations against corruption of their administration and the integrity of officials.

A public official includes any persons who carry out a public function or who have a public employment status, e.g. civil servants, employees of public or government services, regardless of their function. Employees of entities may also be public officials if the entity is established under private law but is, for example, majority state-owned or state-controlled. A more detailed definition of public official is provided in the **ABC and Sanctions Guidelines**.

It can sometimes be difficult to know whether one is dealing with a public official or an employee of a private firm. There are many enterprises in the healthcare sector which are state-owned or which perform public functions; representatives of these organizations are to be treated as public officials. Maximum restraint is thus called for in dealings with individuals from such organizations, in particular with regard to giving gifts and invitations. Please consult the **ABC and Sanctions Guidelines** for more information concerning dealings with public officials.

3.4. Bribery of employees of private enterprises is illegal

It is also a criminal offence in most countries to offer, promise or give any advantage or value to an individual in the private sector in order to induce them to act improperly or to reward them for doing so.

For example, improperly influencing procurement decisions by providing benefits to decision-makers or related parties is illegal, even if these decision-makers are employees of a private-sector enterprise.

This applies to influencing employees of organizations or other individuals in connection with our business anywhere in the world.

3.5. Invitations and gifts to and from private-sector customers

This sub-section applies exclusively to private-sector customers, and in particular to contacts with representatives of customer firms who are not public officials or acting on behalf of a government organization.



Making invitations or granting gifts to, or receiving invitations or gifts from, such persons can be customary in business relationships. For the purposes of the Code of Conduct, an 'invitation' constitutes any request to participate, for example in an event or in hospitality, and a 'gift' is anything given voluntarily without payment in return, notably to show favour toward someone, honour an occasion, or make a gesture of friendship.

An invitation to an event must be granted or received as a matter of courtesy, its value must be reasonable and appropriate under the circumstances, it must be in line with business standards and the **ABC and Sanctions Guidelines** and it must not be perceived as an attempt to influence or bribe.

A gift must be granted or received as a matter of courtesy, its value must be reasonable and appropriate under the circumstances, it must be in line with business standards and the **ABC and Sanctions Guidelines** and it must not be perceived as an attempt to influence or bribe. A gift cannot comprise a monetary payment. Because gifts are given directly to customers, in case of doubt their value should be set conservatively so as to avoid creating any impression of attempting to influence.

You must consult the **ABC and Sanctions Guidelines** for more detailed rules and approval requirements in relation to invitations and gifts.

3.6. Treatment of discounts, commissions and consultant contracts

a) A discount is a price reduction granted to a customer against generally announced or official prices or factory wages. A discount may also be granted through providing additional products or services, or in other ways.

Discounts are granted exclusively between parties to a written contract, i.e. generally the Synlab Group and the customer/contract partner. Thus the parties who have authority to grant discounts are the Synlab Group company representatives who are responsible and accountable for the conclusion of the underlying contract. Internal Synlab Group company policies authorizing only certain managers to grant discounts remain unaffected.

The beneficiary of a discount is always our contract counterparty. It is prohibited to grant a discount in the form of an economic benefit to a third party, such as an employee of the contract partner's organization, rather than to the contract partner itself as a firm.

Discounts must never be offered in exchange for personal benefits.

b) A commission is a payment for brokering a transaction. We only pay commissions to third parties (commission recipients) for arranging a contract transaction with a customer which is in Synlab Group's interest. For any arrangement under which a commission is paid, there must be a contract in writing.

The commission recipient may not be a shareholder, executive or employee of the customer/contract partner in the brokered transaction, nor working for the customer/contract partner in an employee-like relationship (e.g. freelancers, consultants of the customer).

Particularly with international business, the appropriateness of commissions must be carefully monitored so as to rule out illegal forwarding of commissions to decision-makers within the customer's organization or to public officials.



In business practice, careful distinction should be made between granting discounts and paying commissions, which must always be strictly separate; discount payments to customers may not be re-characterized as commissions to third parties or represent concealed commissions, and conversely, agent commission claims cannot be utilized for price reductions in sale or other contract negotiations.

In considering the amount of agreed discounts or commissions, amounts customary in commercial practice in the business area concerned should be referenced, factoring in the significance of the overall transaction to both the customer and the Synlab Group. When negotiating a commission, the probable significance and expected amount of effort by the agent in brokering the prospective transaction are to be considered. The precise nature and scope of services to be rendered by the agent must be set out in writing, and such agents must be subject to appropriate due diligence in line with Synlab's internal controls.

Applicable laws must be observed when negotiating discounts and commissions, including specifically the requirement of documenting such transactions and respecting limits of appropriateness.

c) To the extent that any Synlab Member engages a consultant, there must be a contract in writing setting out the arrangements between the parties including the precise nature and scope of services to be rendered by the consultant. These consultant contracts may only be concluded with persons or companies working for and in the interests of the Synlab Group. Just as with commissions, careful attention must be paid to the appropriateness of consultant fees so as to rule out the possibility of a portion of the fees being forwarded to a shareholder, executive, employee or other representative of the customer, or to a public official. Consultants must be subject to appropriate due diligence in line with Synlab's internal controls. Tax law requires documenting the engagement process and specifying the fee recipient by name, particularly where the arrangement relates to international business.



4. Dealing with suppliers and external service providers

4.1. General rules for dealings with suppliers and external service providers

Suppliers and service providers play an important role in our operations and ability to provide analyses and services to our customers. Accordingly, we select suppliers with special care. Suppliers and service providers are to be selected on the basis of their performance, pricing, suitability for working with the Synlab Group and for their integrity. Suppliers and service providers (including, in particular, any third party that interacts with public officials on behalf of Synlab, or that is engaged to obtain or retain business or business advantages for Synlab) are expected to adopt high standards of conduct equivalent to those contained in this Code of Conduct.

4.2. Provider discrimination is prohibited

Every supplier and service provider who solicits a contract expects an open, fair and impartial process for reviewing bids. Synlab Members involved in contract awarding therefore must observe the following rules:

- providers competing for contracts may not be unfairly discriminated against;
- talks, negotiations and other contacts with providers must be carefully and completely documented;
- Synlab Members must notify their supervising manager in a timely fashion of any personal contacts within a provider's organization which could play a role in the performing of their work; and
- Synlab Members must not provide any information to providers competing for contracts which would, or would be likely to, give them an unfair advantage over other providers.

4.3. Accepting benefits for oneself or a third party is prohibited

Synlab Members may not utilize their jobs to solicit, obtain agreement to or accept benefits for themselves or for third parties, especially in connection with purchasing decisions. Individual Synlab Members may be prosecuted for accepting benefits which are not in accordance with this Code of Conduct or any guidelines or procedures related to the Code of Conduct, including the **ABC and Sanctions Guidelines**, as they could harm the Company's reputation.

4.4. Accepting invitations

Suppliers may invite Synlab Members to functions such as business meals, which can be customary in business relationships. Such invitations may be accepted in accordance with the rules set out in the Code of Conduct, and any guidelines or procedures related to the Code of Conduct, including the **ABC and Sanctions Guidelines**. Invitations must otherwise be declined, making reference to Code of Conduct rules.



5. Competition and antitrust law requirements

The Synlab Group strictly complies with all competition laws (also known as antitrust laws), which are enacted to ensure free and fair business competition. These laws prohibit practices which impair competition, such as:

- collusion amongst competitors regarding prices or delivery of services;
- agreements between suppliers and customers which restrict or prevent competition (such as certain arrangements on exclusivity or the allocation of customers or territories or arrangements in relation to reselling prices); and
- the abuse of dominance (or relative dominance), e.g. unilateral behaviour aimed at restricting the entry or competitive strength of other competitors by unfair means (such as the provision of certain types of discounts or rebates, or excessive or predatory pricing) or boycott.

Competition law also extends to "concerted practices", which consist of direct or indirect, and often informal, contact or cooperation between independent companies.

All EU countries, the US and many other countries have such competition laws, which are frequently applied to international activities of companies. An infringement of competition law entails the risk of investigations, damage to reputation and loss of goodwill, severe fines, damages, invalidity of contracts and – in some countries – criminal sanctions (including prison sentences). In the EU, large fines are imposed against businesses involved in anti-competitive behaviour, which can range up to 10% of the perpetrating firm's global revenues.

Accordingly, particular caution should be exercised when talking with competitors. Competitively sensitive information, which includes non-public information which could be used to alter the recipient's competitive conduct (such as information on costs, current or future charges or strategies) must not be sent to or received from competitors directly or indirectly; even sending or receiving information to/from trade associations must be handled with care. Furthermore, information must never be shared for such purposes as:

- to fix prices;
- to agree uniform contractual conditions or delivery terms;
- to divide up markets, e.g. allocate sales/purchasing territories or customers/suppliers;
- to coordinate or restrict output or capacity; or
- to influence tender outcomes (including by submitting fictitious offers/inquiries).

This does not represent an exhaustive list, but represents some examples of serious competition law infringements as a result of engaging with competitors. As mentioned above, competition law affects not only horizontal, but also vertical issues (e.g. agreements or concerted practices between supplier and customer). Please note that the lines between legal and illegal can easily be crossed in the context of competition law. In case of doubt, please refer the conduct or situation to your Regional Compliance Officer or the Group Legal Department.



6. Ban on involvement in money laundering

Money laundering is the process by which individuals or organizations attempt to hide illegally obtained funds or assets and/or bring these funds or assets back into circulation through apparently legal activities. The Synlab Group is committed to guarding against the use of its business for money laundering, and aims to prevent any attempt to involve the Company or its staff in such activities. Be advised that money laundering and involvement in such activities is a criminal offence which may lead to criminal and administrative liability for individuals as well as the Company.

Anti-money laundering requirements are relevant for every Synlab Member and particularly relevant for Synlab Members in the Finance department (including Accounting and Treasury departments).

Money laundering may not be immediately recognizable as such. You must therefore insist on obtaining clear information for contract partner identification and with regard to payment methods and payer identity.

Synlab Members should be alert to and monitor transactions and situations for any risk of potential breaches of anti-money laundering requirements, and undertake further fact-finding where necessary. This includes monitoring for the following "red flags":

- payments are transacted by third parties who are not contract partners;
- payments are made from an account which is not known to us as a customer account;
- the contract partner seeks to conduct transactions in cash, or using bank drafts, money orders, cashier's cheques or offshore accounts;
- the contract partner refuses to provide trade references or is otherwise reluctant to provide requested information, or provides information which is incorrect or contains inconsistencies;
- payments made by a contract partner do not match agreed contract terms;
- a contract partner requests a payment or refund which is due to it to be made to or through an unconnected third party;
- payments are being split;
- inquiries are made as to whether an amount larger than specified is possible; or
- press coverage indicates that the contract partner or its owners are alleged to have engaged in illicit conduct.

Synlab Members should be alert to any other suspicious circumstances relating to a contract partner or a proposed transaction.



You must comply with the following principles:

"Know your customer", meaning that we only enter into transactions with partners who meet our integrity standards. This requires in particular that you:

- always verify the identity and integrity of prospective customers;
- advise all customers as to our expectations, and review how they respond;
- do not process transactions with customers suspected of conducting improper activities relating to transactions with the Synlab Group;
- carry out enhanced due diligence on contract partners who are Politically Exposed Persons ("PEPs"), or who are owned or controlled by PEPs (a PEP is a person who is, or has, at any time in the preceding year, been entrusted with a prominent public function by a government or international body, and includes family members or close associates of such PEPs); and
- do not accept cash payments of EUR 100 or more (unless otherwise agreed in writing with the relevant Regional Compliance Officer) either in one transaction or in more than one connected transactions.

These guidelines represent general orientation aids only. If you have any doubts about the contract partner or a proposed transaction, you should responsibly and prudently investigate supplier, customer or other third party integrity and the appropriateness of customer activities. You must contact the Group Legal department without exception whenever you have doubts regarding relationships with customers or business partners, or if you have identified payments or activities that are suspicious. This is important because the Group Legal Department may wish to consider whether a suspicious activity report should be filed with the relevant authorities in specific instances. Unless specifically agreed with the Group Legal Department, you must not tell the relevant contract partner that you have contacted the Group Legal department to raise your concerns where this could prejudice any investigation into the concerns which might be conducted.



7. Economic Sanctions

Sanctions prohibit or restrict financial and trade transactions with targeted persons, entities, governments and countries. They may be imposed by the United Nations or by individual countries and international bodies, such as the United States (US) or the European Union (EU), in order to further foreign policy goals by imposing economic pressure on sanctions targets. Separately, export control laws prohibit unauthorized or unlicensed exports, transfers and sales of certain specified commodities, technology and technical data to certain countries, companies and individuals, as well as (in some cases) re-exports from one third country to another.

The Synlab Group is committed to complying with all applicable legal requirements relating to economic sanctions and export controls. All Synlab Members must comply with all sanctions and export control restrictions imposed, administered or enforced by the United Nations, the US, the EU and other such laws and regulations governing the sale and supply of Synlab's products and services, globally, as may be applicable, including laws and regulations of countries in which Synlab operates in respect of activities within those particular countries, as long as it is not prohibited to do so under applicable anti-boycott legislations.

Compliance with sanctions is extremely important and we take it very seriously. Failure to comply with applicable sanctions may result in reputational, operational, legal and/or regulatory risks for the Synlab Member as well as for Synlab. In many jurisdictions it is a criminal offence to breach applicable sanctions, and breaches can be punished by significant fines and/or imprisonment. Accordingly, you must comply with the rules and approval requirements in relation to sanctions and export controls as set out in the Code of Conduct and in any other relevant guidelines or procedures related to the Code of Conduct, in particular the **ABC and Sanctions Guidelines**.

If you have any doubts about whether a particular transaction or customer relationship is permitted under applicable sanctions or export controls, you must immediately seek guidance from your Regional Compliance Officer before supplying goods or taking any other steps in furtherance of the transaction or relationship.



8. Protecting Company assets and financial integrity

All Synlab Members are responsible for protecting the material and intellectual property of the Synlab Group along with all other Company assets and have a legal obligation to do so. We comply with applicable laws and regulations, including International Financial Reporting Standards (IFRS) and national laws applicable in individual countries. Transparency and accuracy are the foundations of our reporting on activities and results, ensuring that data are always properly recorded and published. Our assets and resources are to be managed prudently.

8.1. Accurate and complete data, documents and reporting

All financial and non-financial reports, documents and data prepared by the Synlab Group must provide a true and accurate view of transactions and events.

This is essential to uphold the credibility and reputation of the Synlab Group both internally and externally, to meet legal requirements and fulfill our obligations to shareholders, Synlab Members and business partners.

Financial data must meet legal requirements and conform with mandatory accounting rules and standards in place throughout the Synlab Group. Gaps and inaccuracies not only violate our standards, but may also violate generally accepted accounting principles and/or applicable laws. There can never be any justification for misrepresenting facts or falsifying records or documents. Those who violate these requirements may face both disciplinary action and criminal penalties.

Accordingly, you must always ensure that:

- all transactions are properly authorized and completely and accurately recorded;
- no unofficial transactions or accounts are conducted or set up;
- internal and external auditors are always given complete and accurate information and access to all requested documents (as permitted by law); and
- you yourself as a Synlab Member demonstrate financial integrity, such as when submitting or signing expense reports.

Under no circumstances is it permitted for you to:

- deliberately record false information in a report, file or expense report;
- falsify documents of any kind;
- exercise disposal over the Company's assets without proper documentation and authorization; or
- attempt to get other Synlab Members to act in any manner which could adversely affect the accuracy documents or accounting.



8.2. Safeguarding Synlab Group assets

All Synlab Members are responsible for ensuring that company assets are not misused or wasted. Assets include Synlab Group property, Synlab Members' work time, proprietary information (including 'intellectual property'), business opportunities, business resources and proprietary equipment items provided for Synlab Members' use.

Synlab Group 'intellectual property' includes patents, copyrights, trademarks and all other forms of confidential business information such as company databases, marketing strategies and plans, research data, technical data, business ideas, processes, strategies and offers (to customers and from suppliers), production costs, competitive pricing, new product development, in-house software, and information, market and customer strategies employed for commercial activities. Protecting Synlab Group 'intellectual property' is important for ensuring the Company's business success, and is therefore a special obligation of all Synlab Members. Every Synlab Member must help protect 'intellectual property', business secrets, other business documents and data carriers from unauthorized third-party access.

8.3. Intellectual property and third-party copyrights

Just as we protect our own business information (see section 8.2), we are committed as well to respecting other parties' intellectual property and protected information.

You should therefore never accept confidential information from third parties nor use it unless doing so is transparently agreed by contract and documented.

Never use materials or data which are copyrighted or otherwise protected unless expressly authorized to do so.

The copying, distribution and selling of Synlab Group information, software and other intellectual property is strictly prohibited.

8.4. IT systems use and security

IT systems and data stored and processed on these systems have a special importance for the Synlab Group of which all users must be aware.

IT systems are for the purpose of gathering and securing Synlab Group intellectual property. IT systems are used for internal and external communication and for storing and using all data and information required by the Synlab Group for day-to-day business purposes. Backing up data and maintaining system operability are thus of paramount importance. Effective security requires cooperation and support from all Synlab Group personnel who have involvement with these systems.

Never use the company's IT systems to forward without permission:

- confidential data on private individuals;
- confidential business information; or
- copyrighted materials.

Never access files or store or upload files which:

- are of a pornographic or otherwise sexually explicit nature;
- promote violence, hatred or intolerant behavior; or
- are of an insulting, disparaging or discriminatory nature.

You must notify the IT departments if you are sent such material on an unsolicited basis.



9. Data Protection

The Synlab Group treats personal data confidentially and strictly complies with all applicable data protection and data privacy laws, designed to protect the privacy of individuals where the Group processes personal data about them. This is particularly important in relation to patient and Synlab Members' personal data, but also applies to personal data relating to the Group's individual contacts at its customers, suppliers and business partners and other individuals.

Personal data may only be collected, processed or used fairly, and only to the extent necessary for clearly specified, legitimate purposes. Processing of personal data also requires a clear legal justification – for example, some processing might be justifiable on the basis of the specific, freely given and informed consent of the individuals concerned; or, in the absence of consent (or where consent is not effective), because it is necessary to comply with a legal obligation or on the basis that it is necessary so that the Synlab Group can pursue its own legitimate interests (although those interests must be balanced against any prejudice to the privacy rights of the individuals concerned).

Personal data must be deleted (or rendered anonymous) when the Group no longer needs it for its legitimate purposes. It must be kept secure in accordance with rigorous data security policies meeting the requirements of applicable law, and appropriate steps must be taken to ensure that it is accurate and, where relevant, up to date. The patients, Synlab Members and other individuals to whom personal data relate must be informed about the Group's processing of their personal data (including specific details such as the data controller, the purpose of the processing, the recipients of the data and potential transfer outside the European Union), and of their related rights, in accordance with the requirements of applicable laws, except in the limited circumstances where legal exceptions to the Group's transparency obligations apply. Individuals also have legal rights of access to their personal data, to correct, restrict or require the deletion of inaccurate personal data and, in some circumstances, to object to the Group's processing of their personal data, which must be respected.

Particular care must be taken when personal data is disclosed outside the Synlab Group and, in particular, third party service providers processing personal data on the Group's behalf must be subject to appropriate due diligence, contractual controls and audit arrangements.

The Synlab Group also abides by other legal requirements and restrictions applicable to the processing of personal data, for example the restrictions on transfer of personal data outside the European Economic Area; the more specific rules regarding health data and data in other particularly sensitive categories; and local requirements to make filings with and/or obtain approvals from data protection authorities.



10. Ombudsman

For certain countries, the Synlab Group may appoint an external lawyer to act as Ombudsman, whose role it is to receive confidential reports on potential violations of laws, the Code of Conduct or any guidelines or procedures related to the Code of Conduct, to review these reports and to forward information to the Compliance Committee as necessary. Where an Ombudsman has been appointed, this will be indicated in the relevant country-specific policy.

Where one has been appointed, the Ombudsman acts on behalf of the Synlab Group, receiving tasks and instructions exclusively from the Compliance Committee, the Chief Compliance Officer or the Legal Compliance Officer. As an attorney, the Ombudsman is subject to statutory client confidentiality.

To ensure confidentiality between the Ombudsman and any informants, the Synlab Group enters into an irrevocable advance agreement with the Ombudsman that no names or any indicative information are to be disclosed to the Company so as to protect the identity of whistleblowers requesting anonymity.

The Ombudsman accepts information regarding potential violations of laws, the Code of Conduct or any guidelines or procedures related to the Code of Conduct by telephone, letter, e-mail and in personal meetings. The Ombudsman reviews the reports for plausibility then decides the further course of action based on the credibility of the information and of the informant, the nature and seriousness of the offence and the potential impact on third parties and on the Synlab Group.

The Ombudsman then forwards the information to the Chief Compliance Officer or the Legal Compliance Officer, presenting the matter and providing a preliminary legal opinion on appropriate further steps.

Upon completion of review by the Compliance Committee, the Ombudsman notifies the informant of the Compliance Committee's findings, taking into consideration the need to protect the interests of any affected parties.

The Ombudsman is a licensed attorney whose identity is made publicly available. The Ombudsman implements appropriate technical and staffing measures to ensure that reports submitted reach him/her personally or one of the representing attorneys at his/her office by the next business day.



SYNLAB Limited
4 Devonshire Street
London W1W 5DT
United Kingdom

www.synlab.com

© 2017 SYNLAB Limited

No liability for errors, mistakes and incorrect price data. Changes reserved. All texts, images and contents are under copyright of SYNLAB Limited.

As of 1 / 2017