MEDIOBANCA
INTERNATIONAL (LUXEMBOURG) SA

Mediobanca International Board of Directors of 27 July 2022

Code of Conduct

July 2022

MEDIOBANCA
INTERNATIONAL (LUXEMBOURG) SA

Contents

1. The Code of Conduct: a shared commitment

The Code of Conduct (hereinafter also referred to as the "Code of Conduct" or "Code") is the document which, along with the Code of Ethics, sets out the fundamental principles on which Mediobanca International's (hereinafter also referred to as "MB Lux" or the "Bank") and Mediobanca banking Group's (the "Group") reputation is based. It contains the values underlying its everyday operations and it describes the standard of conduct required from all staff and collaborators.

Approval and publishing

MB Lux's Board of Directors approves the Code and its significant updates in line with the Group Regulations.

Recipients are notified via e-mail upon the Code of Conduct publication.

Individual responsibility

All the staff and collaborators, including suppliers and consultants (the "Recipients"), of MB Lux must familiarize themselves with the Code of Conduct and have their behaviour driven by the principles and values set out herein.

Recipients must also:

- Comply with external and internal regulations applicable to their own activities;
- Attend to all the trainings undertaken by the Bank on relevant regulations;
- Foster the spreading of an ethical culture by being a positive example to other colleagues;
- Report promptly any breach and co-operate in the inquiries.

The heads of organizational units must ensure that Recipients under their supervision act under the highest ethical and professional standards.

If they do not carry out their powers of supervision with due care, they may be held jointly responsible for the breaches committed by their own staff.

Reporting breaches

If Recipients believe in good faith that there has been a breach of the Code of Conduct, or if there is a concrete risk that such a breach will occur, they have to promptly contact their line manager and/or report the issue by writing an email to the following address: whistleblowing@mediobancaint.lu
Such reports are analyzed quickly and dealt with the utmost confidentially, ensuring the whistle-blower is not subject to discrimination or retaliations as a result.

Luxembourg financial Regulator, the CSSF, has also implemented a channel to collect reports coming from regulated entities' staff and collaborators to be used after having activated the internal whistleblowing channel.

Q. Do I have to report breaches referred to other Bank's units or other Group companies?

A. Yes, since unprofessional and unethical conduct may jeopardise the trust placed in the Group by its customers and the other stakeholders, as well as entailing possible legal consequences.

Q. What should I do if a colleague asks for my support in an activity which in my view is contrary to the Code of Conduct?

A. All the Recipients must refrain from any kind of conduct potentially contrary to the Code of Conduct and report any possible critical issues through the channel available for this purpose.

Duty to co-operate

Authorities or internal control units may perform audits or inquiries to examine potential breaches of internal or external regulations.

If the Recipients are involved in these inquiries, they must co-operate with the utmost transparency, providing truthful, complete and accurate information. Further, in case of requests or inspections by the authorities, they must:

- Ensure the utmost confidentiality on the authorities' requests and on issues discussed;
- Avoid comments or judgments based on personal impressions or not related to their role;
- Not seek nor offer advantages of any kind to obtain favorable treatment;
- Inform promptly whichever unit is responsible, from time to time, for coordinating relations with the authority;
- Promptly inform the unit in charge of coordinating relations with the authority of any request, abide by any instructions given by that unit and draw up minutes of any meeting with the authority.

Q. I received a call from a regulatory authority regarding inquiries into a transaction which I closed with a client. May I answer their questions?

A. Yes, but only if you involve the internal units responsible for relations with authorities (e.g. internal control units or specialized units). You shall also pay attention to frauds attempted by persons pretending to be public officials, especially through phone calls.

Consequences of breach of the Code of Conduct

The Code of Conduct is an integral part of the internal regulations which every Recipient is bound to comply with, including in accordance with their own position or collaboration contract.

Breach of the Code of Conduct and of the internal regulations may impact variable remuneration and result in the application of disciplinary sanctions commensurate with the seriousness, the extent (including whether the infringement is repeated) and the external relevance of the breach committed, including dismissal. If the Recipient's conduct constitutes unlawful behavior, this will be also reported to the relevant Authorities.

2. Core values

The Group and Bank's priority interest is to promote an ethical culture which is based on the principles of proper conduct, professionalism, customer care and responsibility.
Sharing these values means to honor the trust that has been placed at Group's level and to preserve its excellence. Recipients have the shared responsibility for maintaining and promoting the highest standards of ethical conduct with all parties they come into contact.

PROPER CONDUCT ✓ Act in accordance with the external and internal regulations. ✓ Do not compromise integrity and honesty in order to achieve an economic interest. ✓ Maintain relations with counterparties based on loyalty and honesty.	**PROFESSIONALISM** ✓ Improve your professional skills on an ongoing basis. ✓ Foster an open and inspiring working environment which nurtures talents.
CUSTOMER CARE ✓ Offer clients an outstanding service which anticipates market trends. ✓ Do your job considering the client's best interest as your top priority, earning and preserving their trust. ✓ Ensure the utmost secrecy to confidential information.	**RESPONSIBILITY** ✓ Consider the economic, social and environmental impact of your decisions. ✓ Protect and enhance continually the Group's reputation.

Proper conduct

Proper conduct means always doing the right thing and never compromise to achieve an economic interest.

The Code of Conduct provides guidance on many critical aspects of our working activity, but it is not meant to be an exhaustive guide on each of the Group's regulatory obligations. It expresses the core values and fundamental principles of the Group's compliance culture. Therefore, if the Recipients are facing a situation that is not expressly addressed by the Code of Conduct and other internal regulations, they shall ask themselves the following 5 questions to determine which is the proper course of action:

- Is it compliant with external and internal regulations?
- Is it compliant with the principles set out in the Code of Ethics?
- Am I sure it could not be perceived as inappropriate or unprofessional?
- Am I ready to take responsibility for the consequences of my actions?
- Am I sure it could not cause damage in any way, including reputational, to the Bank or its stakeholders?

If the answer to each question is positive, you may go on with your action. However, if even only one answer is negative, the behavior could breach the Code of Conduct.

If Recipients have any doubts, they may contact Compliance Unit to ask for support.

Professionalism

Professionalism means improving your professional skills on an ongoing basis. To achieve this, Recipients must understand and comply with internal regulations applicable to their area of operations, attend training initiatives planned by the Bank and ensure that they satisfy requirements and certifications required under external regulations for their position.

Professionalism also develops thanks to an inspiring working environment that values individual skills, imbued with mutual trust and cooperation and based on respect for everyone's personality and dignity. Therefore, Recipients shall promote a working environment open to discussion and diversity, free from any discrimination or retaliation.

Customer care

The Group and the Bank make customers its first priority, therefore Recipients shall at all times ensure that customers take free, informed and aware decisions and that the services and products offered satisfy their needs.

Recipients shall prevent or manage, by protecting their clients' interests at best, potential conflicts of interest, even if only apparent, which may raise upon their working or personal activities.

Recipients shall treat customer information with confidentiality, ensuring that it is processed in a way that guarantees its integrity and prevents its destruction or dissemination.

Responsibility

The Group respects the cultures which are present in the countries where it makes business and wishes to contribute to their economic and social development through its business activities.

By adhering to "The Ten Global Compact and Responsible Banking Principles" promoted by the United Nations, the Group upholds and applies fundamental principles about sustainable development, human rights, working standard, environment protection and fight against corruption and tax evasion, with the aim of creating an economic, social and environmental framework fostering a healthy and sustainable economy. By supporting volunteering initiatives, the Group is providing a service to our communities and we encourage our Recipients to do the same, by supporting their commitment.

Within the general compliance to Global Compact principles, the Group pays specific attention to diversity and inclusion issues, with the aim of promoting each individuality in a long-term sustainable growth perspective.

Recipients shall therefore be aware of the risks that their actions may entail, also in the long term, and be able to manage them properly. These risks include social, environmental, and reputational risks, which may also stem from personal activities.

3. Protecting the customer's interests

The Bank obtains the customers' trust by focusing on the protection of their best interests in the long period and by trying to anticipate their needs with an excellent array of products and services. All customers relationships are driven by the general principles of diligence, proper conduct and professionalism.

Transparency is at the heart of the Group's relations with its customers. Recipients shall always pay the utmost attention to their customers' interests, show proper care and professionalism, and comply with all applicable internal and external regulations.

Marketing and communication towards customers

Recipients shall provide potential customers with clear, correct and exhaustive information on products and services offered to allow them to take informed and aware decisions. Therefore, Recipients shall be familiar with all the products and services that may be offered.

Information shall be provided in simple language before any formal agreement and shall allow the customer to understand clearly the features of the product/service, its risk, price and components thereof and its expected performance.

Recipients shall not provide any information that is untrue or could mislead potential customers on the characteristics of the product/service. They shall not guarantee future results nor investment performances, save where these elements are defined in the contracts.

Recipients shall promptly inform their line manager of any fraud, even attempted, against customers or third parties and line managers shall involve the Group Audit Unit for relevant in-depth analyses.

Q. May I provide to the customer (or prospect customer) all the information on the products and services, but without providing them with the dedicated documents drawn up by the Bank? Or provide the information only after the customer makes a transaction?

A. No, as information on products and services shall be rendered to the customer in advance and by using the documents drawn up by the Bank, to allow them to take an informed decision. The contents of the documents provided to the customer in a durable medium are to be described to them also by the banker with a clear and detailed explanation.

Product manufacturing

When manufacturing a product, Recipients shall analyze its features to define the type of clients to whom the product may be offered or recommended (so-called target market) and a consistent distribution strategy.

The target market shall be defined taking into account the customer's financial sophistication, experience, risk appetite and needs, as well as the time-horizon of the investment.

Relevant documents for each product shall include clear and exhaustive information on the product's feature, pricing mechanisms and risks, including potential conflicts of interest.

Recipients shall monitor manufactured products to ensure that they satisfy the target market's interests on an on-going basis and adopt any action that may be necessary to prevent damages to customers from happening.

Third-party distributors

When a third party distributes the product manufactured by the Bank, Recipients shall check such third party's reputation, experience and internal procedures before signing any commercial agreement. These agreements shall require information flows between the third party and the Bank and the compliance by each party with the relevant regulatory obligations.

Cost, charges and inducements

When providing investment and ancillary services, Recipients shall provide the clients with information on the applicable costs and charges, and on inducements received/given from/to subjects other than the client.

Recipients shall also provide the client with the product costs of products either recommended or offered for sale.

Usury

The customers' best interest shall not be jeopardized to achieve a greater economic return. National regulations set detailed limits to interest rates that may be applied to loans.

Customer requests and complaints

During the relationship with customers, Recipients shall be available to answer to any information or clarification requests from customers on products/services in a clear and prompt manner.

If a customer is not satisfied with the product/service and files a complaint, Recipients shall immediately inform competent units and comply with any instruction received. Complaints shall be managed in a sensitive and professional manner and will be considered an opportunity to further improve and increase customers' trust and satisfaction.

Cross-border services

Cross-border provision of services (to customer residing in a country different from the Bank) may trigger regulatory requirements set by the country where the customer resides. Recipient shall ensure that the Bank is authorized to perform its business activity also in the country where the customer resides and comply with such country's relevant regulations.

4. Protection of information

Protecting processed data is the key to the Bank's success, since destruction, disclosure or unauthorised access to such information may create significant economic or reputational damages.

Anytime the Recipients access, record, transfer, delete or disclose information, they must take great care to protect such data from rom unauthorized destruction, loss, modification, access, and disclosure.

Information security

Most information is processed through IT instruments, therefore some important principles must be followed to grant security to such data.

The only authorised channel to process data is the Bank's IT systems (including the corporate mail address). Corporate systems and devices shall be used only for professional purposes, while personal devices are not to be used to process information for professional purposes.

Each communication that travels on the Bank's systems shall comply with the principles set out in this Code of Conduct. Since all information is transmitted through corporate IT systems, the Bank is allowed – within the limits set by applicable regulations – to record such communications and analyze transmitted data.

Recipients shall store and use their credentials to access IT systems as prescribed by internal regulations and block their corporate devices (computers and smartphones) when they are temporarily away from them. Further, they shall follow any guidance provided by the Bank in order to protect data from external threats.

Q. May I use my corporate e-mail address also for personal purposes?
A. No, corporate IT systems shall be used for professional purposes only. However, internet and web-mail services use for personal purposes is tolerated, as long as it does not interfere with you regular working activities and you comply with the Code of conduct principles.

Q. A person who says to work for the Service Desks is requesting personal or confidential information (e.g. login credentials to the corporate mailbox or to a corporate application) from me. May I satisfy their request?
A. No. It is forbidden to provide login credentials to anyone, including Service Desk personnel. If someone asks them from you, you shall reach Service Desk through the official channels and the relevant units as prescribed by the internal regulations.

Protection of confidential information

Confidential information includes anything that is not generally known to the public on Mediobanca, the Recipients themselves, customers and other counterparties.

Recipients shall process confidential information only when authorised by applicable regulations or by an agreement with the data subject.

Recipients shall protect confidential information from the time of its creation to the moment where it becomes public or is destroyed and shall process it only within the authorized channels. In particular, the Recipients:

- Shall process confidential information only for purposes connected with their business activity and process only the minimum amount information necessary to achieve these purposes;
- Shall not process confidential information in public places or if there is a risk of involuntary disclosure to third parties (e.g. in public places);

- May communicate confidential information only when required by law, a regulatory authority or an agreement and if the Recipients have a legitimate need to process the information for their professional activity (e.g. other colleagues or advisors);
- Shall inform anyone who is aware of the information of its confidential nature and of the duties deriving therefrom beforehand, also requiring that a non-disclosure agreement consistent with the internal standards be signed if the recipient is outside the Bank;
- Shall ensure that confidential documents are stored or destroyed in a way aimed at excluding the possibility of unauthorized access (e.g. clean desk rule, encrypting a file with a password).

Information shall be processed only through the corporate channels: Recipients shall not use personal e-mail addresses nor online storage services to treat confidential information.

Q. Can I send working documents to my personal email address, should I need to take part to conference calls during my holidays?

A. No. Sending confidential information to personal email accounts is forbidden, unless in exceptional cases. Remote access to corporate e-mail accounts is allowed only for Recipients who have personal devices that have been specifically approved.

Q. A client sends me digital confidential documentation. May I store them in a shared folder?

A. Yes, but the shared folder shall be accessible only to colleagues covering the transaction.

Recipients must inform Compliance unit as soon as they know or have reasonable grounds to suspect that a confidential information has been used or sent without authorization and they must abide by any guidance received.

Q. I have been provided by mistake with credentials to access an online folder containing information on a transaction which I am not working on. What should I do?

A. You must immediately request that your authorization be revoked from the person who has provided it and you must inform Compliance Unit.

Q. I wrongly sent an email to a client with confidential information on another customer. What should I do?

A. You shall recall the e-mail if possible. Otherwise, you shall inform the recipient that information is confidential and request them to delete it immediately. In any case, you must inform immediately Compliance Unit, which may request further actions from you.

Inside information

Mediobanca S.p.A. (the "Parent Company") and MB Lux maintain specific lists containing information on all persons who – by reason of their activity or role – have or may have access to information that directly or indirectly regards Mediobanca, other financial instruments issuers, or financial instruments, and which is:

- Confidential, but may become inside (watch lists);
- Inside information (precise information on which, if made public, would likely have a significant effect on the prices of a financial instrument – insider lists).

The person responsible for the transaction must open such lists promptly, and include anyone having, also potentially, access to the information as soon as possible. Recipients who hold such information (and are therefore inserted in the watch or insider list) and communicate it to anyone else under the *need-to-know* principle must inform them about the nature of the information and notify the person responsible for the transaction so as to allow them to include such persons in the list.

Hence, Recipients who receive this information, without being notified of the inclusion into a watchlist or an insider list shall promptly get in touch with the person responsible for the transaction to make sure that they have been included in the list.

Recipients who are included in a watch list or in an insider list must not, for their own account or for the account of the Bank or of a third party:

- Deal in the interested financial instruments;
- Disclose information to third parties outside the normal exercise of their activity;
- Inducing other persons to deal in the interested financial instruments.

Q. May I execute transaction for the Bank's account on financial instruments if I have inside information on them and I have acquired it outside my working activity?

A. No, because that would amount to insider trading.

Q. A colleague, who was included in the insider list, has been transferred to a different office. As his involvement in the transaction is not envisaged anymore, may I delete him from the insider list?

A. No, as the insider list shall include any persons having inside information. Therefore, the colleague has to remain in the list, with indication provided of the date on which he ceased to have access to inside information.

Information barriers

The Parent Company has set up physical, organizational and IT information barriers to limit potential insider dealing activities and to minimize the risk of conflicts of interest. The barriers separate:

- Private areas, which typically generate or process inside information (divisions offering corporate and investment banking services such as lending and capital markets); and
- Public areas, which typically do not process inside information (sales and trading staff, research analysts and private bankers).

The Recipients shall in any case ensure that allowed contacts between private and public areas are trackable so as to make their legitimacy easier to demonstrate in case of controls (including inquiries from the authorities).

Personal data protection

Recipients shall process personal data related to colleagues, customers and counterparties in full compliance with the principles of lawfulness, fairness and transparency. In particular, personal data must be:

- Collected and processed for specific, explicit and legitimate purposes;
- Kept accurate and up to date;
- Retained for no longer than it is necessary for the purposes for which the data are processed;
- Processed in a manner that ensures their security.

You may contact the Data Protection Officer (dpo@mediobancaint.lu) for clarifications on the EU regulation on personal data (GDPR).

Q. May I process a customer's personal data with a purpose different than what was declared when I collected them?

A. No, you may process customers' personal data only within the limits set out by the data protection information notice that has been provided to them.

5. Market integrity

MB Lux Mediobanca protects the integrity of financial markets and free competition.

Financial markets integrity

In order to protect market integrity, Recipients:

- Must not engage in any conduct that may alter, also in a relevant way, the price of financial instruments (e.g. by fake news or fake trades);
- Must strictly abide by the markets which they access to trade and keep an up-to-date knowledge of market rules.

At Group level, in order to protect the Group from being inadvertently involved in market manipulation or insider trading made by clients, Recipients shall record and store every order they receive and monitor client trades to detect any suspicious transactions that have to be reported to Compliance unit.

Anti-competitive practices

Recipients must not, even in agreement with other market participants:

- Raise or fix arbitrary prices for products or services;
- Rig or fix the amounts of bids made in open bidding processes;
- Divide up clients, geographical areas, markets or products;
- Restrict or cancel the offer of products or services;
- Damage the image of a competitor with the general public, or disclose confidential information on a competitor to third parties;
- Refuse to engage in commercial relations with specific counterparties.

Generally, Recipients are not allowed to share any sensitive information or information which is property of the Group with competitors if such information is not public (including data on prices, discounts, increases, reductions, clients lists, production costs, quantities, turnover, sales, marketing and investment plans). Such disclosure may be deemed a breach of competition rules and entail fines for the Bank and for the individuals involved.

An example of anti-competitive practice is the use of multilateral chats by traders from multiple banks to exchange information on prices and volumes offered in the pre-auction period and on prices shown to clients or to the market.

Particular attention must be paid to the contractual clauses which may restrict the freedom of the customer to enter into contracts with other financial intermediaries, e.g. by granting

the Bank a pre-emption right in offering the client products/services different from those regulated by the specific agreement.

Personal dealing

In order to prevent personal dealing from entailing, also only apparently, conflicts of interest or use of confidential information, Recipients must not trade for their own personal account:

- In financial instruments issued by companies on which the Recipients have confidential or inside information;
- As counterparty to the Bank or to a customer;
- In the form of naked short selling;
- In cryptocurrency;
- In Mediobanca S.p.A. instruments in the days immediately close to the publication of the periodic financial statements;
- In financial instruments issued by MB Lux in the days immediately close to the publication of the periodic financial statements of the Parent Company;
- For speculative purposes, meaning acquisitions made in which the instruments concerned are resold on the same day;
- If the trades amount to more than 20 in a calendar month;
- In instruments that have been subjected to a temporary trading ban issued by Compliance unit;
- If the trades are able, through personal hedging strategies or insurance policies on salaries or other items, to alter the alignment of remuneration mechanisms with equity content with company risk.

Internal regulations also provide for:

- Additional bans which are applicable to particular categories of Recipients;
- An obligation to report allowed personal transactions within 10 working days of the trade.

Personal dealing bans and obligations apply also to related persons (individuals who trade on behalf or to the benefit of the Recipients, who are joint-holders with Recipients, or authorised to trade on accounts held by the Recipients) and to Recipients when they trade on behalf of third parties.

Q. Can I sell shares of an Italian listed company I bought during a previous working experience.

A. It is possible to sell the shares, but you shall notify the Compliance Unit.

6. Managing conflicts of interest

MB Lux identifies, prevents and manages situations of conflicts of interest, which may harm the interests of a customer or of the Bank to benefit of a third party.

It is not acceptable to favour one customer over another.

Recipients must insert all relevant information on business opportunities in which they are involved in the Bank's IT systems, to make potential conflicts of interest detectable in a timely manner. If they are aware of a situation of potential conflict – also of a personal nature – Recipients must report it to Compliance unit immediately and abide by any guidance received.

Based on the materiality of the potential conflicts, the Bank has approved a Policy which, among other things, identifies standard measures (e.g. information barriers) and additional measures for specific situations able to mitigate the risk of damaging clients' interests.

Recipients must therefore, in accordance with the methods described in the internal regulations, promptly report any situation involving a potential conflict of interests – including of a personal nature – and comply with the possible additional measures recommended by the Compliance unit.

In particular, Recipients must not be led by inducements from third parties to place products that are not suitable for the client's knowledge and profile.

Q. Which are the types of conflicts that come into relevance?

A. Internal regulations cannot identify potential conflicts that are most likely to happen due to the Bank's business. However, since it is not possible to identify any potential conflicts beforehand, if Recipients think they have found a potential conflict, they shall inform Compliance unit immediately.

Setting up separate teams

In acquisitions managed through competitive bidding processes, MB Lux may offer its services (also through dedicated business units of the Parent Company) to more-than-one bidder to finance the transaction and/or structure the related derivatives, insofar as dedicated teams, suitably segregated to maintain the confidentiality of the various bidders' information, are set up within the business units involved.

Personal conflicts of interest

Recipients must report any conflicts with their own personal interests to their respective line managers and the Compliance unit, to ensure that the necessary mitigation measures are taken correctly and promptly.

Recipients shall also request specific authorization before acquiring any personal interest such as in not-listed companies and positions in companies outside the Group (i.e. outside business interest).

Q. What should I do if a company owned by one of my dearest friends contacts me for a potential business opportunity?

A. You shall inform your line manager and Compliance unit immediately to assess any potential action to take, since personal relationships with potential customers or counterparties may create conflicts of interest.

Q. I sit in the board of directors of a company and I have been asked to become their chief executive officer. Shall I request a new approval?

A. Yes, because a new approval is required anytime a change in a previous personal interest may increase the risk of conflicts of interests or reputational impacts on the Bank happening.

7. Tackling bribery and corruption

The Group acquires and maintains commercial relations solely on the basis of its own excellent services offering and clients' specific needs, and rejects any conduct which is (or could be) intended to obtain or to offer an improper advantage.

In order to ensure full compliance with the regulations on bribery and corruption, Recipients must not:

- Offer or promise – even indirectly – cash or any other valuables with a view to obtaining an improper or unjust advantage;
- Accept cash or other utilities to breach their own duties towards the Bank.

The notion of other utilities includes any item of value, including invitations to events, gifts, travel/lodging/food expenses, fees and job/collaboration/internship opportunities.

Facilitation payments made in order to speed up an administrative process, even without influencing its outcome, are also prohibited.

Risks of bribery and corruption are also managed through the due diligence procedures for the selection of the Bank's suppliers.

Finally, when structuring and performing transactions and when signing commercial agreements, Recipients shall assess the potential legal and reputational risks associated with bribery and corruption, also taking into account the reputation and the country of residence of all parties involved.

Q. One of my clients has suggested his nephew for an internship opportunity in MB Lux. What should I do?

A. Offering an internship, even if it is unpaid, falls within the "anything of value" definition, hence HR must be informed of the link with the candidate and you must refrain from exerting improper influence in the hiring process.

Gifts

The exchange of gifts during holiday season or upon particular anniversaries is a customary practice that may foster goodwill in business relations.

However, gifts which – due to their features or circumstances – may appear to have been made with the intent of improperly influencing the independence of judgment and conduct of parties involved, thus exposing the Bank to the risk of breaching anti-bribery applicable regulations, should be avoided.

Furthermore, specific approval processes shall be followed for gifts whose value exceeds set thresholds or which may have deemed as relevant under compliance purposes, following a self-assessment test. Particular attention must be paid to gifts to the public administration.

Q. If I wish to pay myself for a gift to one of my clients for his/her birthday, does the internal regulation still apply?

A. Yes, since if the gift is related to the relationship between you and one of your customers there still are the same bribery and corruption risks.

Q. A client whom I assisted in the past for a transaction has a bottle of wine – the value of which is about 50€ – delivered to me in August. May I accept it or are authorisations required?

A. If the outcome of the self-assessment test is that: i) the counterparty does not belong to the public administration, ii) the gift is not received during the course of an ongoing negotiation and iii) no more than two other gifts were received from the same counterparty during the last 12 months, the gift may be accepted without requesting for an authorisation.

8. Anti-money laundering and counter-terrorism financing

The Bank contributes to safeguarding the economic and financial system, by adopting procedures and controls to prevent the products or services offered from being used improperly to facilitate money-laundering and terrorist financing.

All the Recipients are prohibited from participating in or facilitating any acts of money-laundering or terrorist financing, which could result in fines or penalties against the Recipients and the Bank, as well as in reputational damages.

Therefore, the Recipients – before starting any business relationship or executing any transaction – shall identify their clients and beneficial owners (individuals owning or controlling the customer) and collect information requested by the internal procedure to assign them a risk profile that drives the intensity and depth of the customer due diligence activity under the external and internal regulations.

Particular attention shall be paid to starting and managing commercial relationships with parties linked to high-risk jurisdictions, especially if subject to national or international restrictive measures. These regulations indeed set specific limits to allowed transactions and such limits shall be assessed by Recipients and Group AML to ensure the compliance of the intended business activity.

Recipients shall also monitor, adopting a risk-based approach, their own clients' transactions in order to promptly inform the Compliance Unit when they know, suspect or have reasonable grounds to suspect, that money-laundering or terrorist financing activities are occurring, have occurred or have been attempted, in order to assess whether to make a report to the relevant Authorities.

Q. If I identify a potentially suspicious transaction after it has been executed, am I required to report it in any case?
A. Yes, because the suspicious nature of a transaction could become clear only after it has been completed, also by taking into account the subsequent behaviour of that client. Hence Recipients shall notify their line manager and the Compliance Unit of any potentially suspicious transaction as soon as they become aware of it.

Q. May I perform a transaction if I know that the customer is acting on behalf of someone subject to assets freezing under international sanctions?
A. No, making funds available to individuals subject to assets freezing measures is forbidden. Therefore, each Recipient shall report such transactions as soon as they are aware of them.

Q. May I participate in projects or deals involving (in any capacity, and also indirectly) a country subject to restrictive measures?
A. No, as such activity may entail a breach of applicable regulations regarding commercial and financial sanctions. Therefore, each Recipient shall inform immediately the Compliance Unit for an assessment of the transaction.

9. Combating tax evasion

MB Lux adopts a "zero-tolerance" approach towards any conduct aimed at pursuing tax evasion. MB Lux also contrasts conducts facilitating tax evasion, which may be put in place by employees, collaborators, suppliers and, in any case, by any subject operating on behalf of the Bank.

Recipients must:

- Not knowingly assist the Bank's clients or counterparties intending to put in place tax evasion in any country;
- Not ignore the conduct held by the Bank's clients or counterparties clearly aimed at achieving illegal tax savings in any country.

The notion of tax evasion includes any conduct aimed at achieving illegal tax savings, by being knowingly involved in, or through acts aimed at, fraudulent tax evasion.

The notion of facilitation of tax evasion includes any conduct aimed at knowingly facilitating the implementation of tax evasion and applies to any subject operating on MB Lux's behalf, including employees, collaborators and suppliers.

Risks related to tax evasion and facilitation of tax evasion can be managed, inter alia, through due diligence processes over suppliers, and through assessing potential legal and reputational risks related to tax evasion that arise while structuring and managing transactions.

Q. A client asked me to assist them in structuring a transaction which in my view might be aimed at, among other things, achieving illegal tax savings. What should I do?
A. The Compliance Unit must immediately be involved. Ignoring the clients' conducts aimed at tax evasion, or deliberately facilitating them, may lead to civil and criminal liability.

10. Managing reputational risk

Mediobanca Group's outstanding reputation, based on the observance of its core values, is an extremely valuable asset to be safeguarded, in the sense that its damage could have long-lasting consequences which would be difficult to remove.

Recipients must always consider the impact of their conduct on the Bank's reputation, taking also into consideration the risks related to the clients, the counterparties and the transactions carried out.

Relations with customers

Associating the Bank's name with potential clients and counterparties that are involved in unlawful or non-transparent conduct may have material reputational impacts on the Bank.

In view of the possible consequences in reputational terms, the Recipients should not enter into relations with parties that - based on public data or on information known for work-related reasons - are not aligned with the Bank's reputational profile.

In the course of the relationship, Recipients are in any case required to promptly report to the Compliance unit all up-to-date information on the client that could have a reputational impact on the Bank.

Q. A former client, would like to carry out some operations. Should I perform reputational checks, even if the potential counterparty was a client for many years?
A. Yes, reputational checks must be repeated if the client does not have an active commercial relationship with the Bank, even if in the past he/she has been a client.

Newspaper rule

Recipients should pay the utmost attention to the form and content of their documents and the communications they engage, imagining the effect these might have if made public on the front-page of a famous newspaper (the so-called "newspaper rule"). Negligence and inaccuracy in communication could indeed lead to a misinterpretation of the content which may sound improper.

Q. Does the "newspaper rule" apply even to emails sent to my colleagues as part of my working activities?
A. Yes, even emails sent internally could be misused if made public.

Personal activities

Recipients shall refrain from any conduct that may compromise their integrity and honesty, also outside working activity, as it may have a negative impact on the Bank's reputation. Customers, counterparties and the general public may view the Recipients as representing the Bank even when they are not performing any work-related activity.
Personal use of social networks shall also comply with the Code of Conduct principles, taking into account that editing and deleting contents that have been published may face technical difficulties.

Reporting of material events

Recipients must inform immediately the Compliance unit if they become aware of, or are involved in, an event which could entail a reputational risk for the Bank. Such notification is required if a Recipient, in connection with his own conduct or activity within the Bank:

- Is involved in legal or disciplinary proceedings;

- Is involved in an enquiry, inspection or request by the Authority;
- Receives a complaint from a client or a third party.

11. Use of company assets

Company assets are resources used by the Bank to perform its activity. Protection of these assets allows the Bank to preserve its competitiveness on the market. Hence use of such assets should be based on the principles of integrity, proper conduct and responsibility.

Recipients shall use company assets only for the performance of the professional activity and protect them from being abused, damaged or used improperly, with a view to saving costs and reducing environmental impact.

Recipients shall report any fraud committed or attempted against the Bank promptly to their line manager, who will involve Audit Unit for further analysis.

Security of company premises

In order to prevent damages deriving from negligence or willful misconduct, including by third parties, the Recipients shall grant access to the company's premises only to third parties who have been identified and who are accompanied by an internal representative. In the company's premises, the Recipients may not record audio or video, or take photographs, unless expressly authorized for specific purposes.

Protecting the environment

Mediobanca Group promotes MB Green project, with the aim of ensuring that economic initiative is consistent with environmental requirements. It includes:

- Monitoring how resources are used and limiting the amounts of resources used;
- Improving energy and waste management;
- Maintenance of property and systems;
- Raise awareness on the responsible use of resources.

Travel expenses

Transfers are essential for business, but the Recipients shall ensure that the duration of the journey and the amount of the related expenses are limited, without compromising the effectiveness of the mission, and shall always provide sufficient documents corroborating expenses incurred.

12. Communication and powers to represent the company

The Bank ensures clear and exhaustive disclosure of all information to enable counterparties to take aware decisions, and guarantees transparency, both internally and in relations with third parties, ensuring that behavior may be traced in order to ascertain that the actions taken have been consistent and appropriate.

Disclosure to the public

The Bank releases data regarding the company's situation by using the appropriate institutional channels and identifying those individuals who are authorised to provide information to the general public and to maintain relationships with the media.
Therefore, Recipients may not, without prior authorization:

- Answer any request from the media or contact them;
- Disclose information on the Bank or related to its activities through social networks or other websites accessible to the general public.

Storage of working documents

Recipients shall store properly all relevant documents, in order to retrieve information easily, according to the requirements of external and internal regulations (generally not less than five years).

Internal communication

MB Lux undertakes to inform all the Recipients of the circumstances and events which could impact their working activity, such as organizational changes or the release of new internal regulations. This communication is to be considered confidential information only for internal use.

Powers to represent the company

The power to represent the Bank is assigned to the Chairman of the Board of Directors, the Chief Executive Officer and staff members expressly entrusted. Recipients shall ensure that they have binding powers and that no further authorization is needed before signing any document on behalf of the Bank.

13. Managing human resources

MB Lux is committed to developing a working environment which valorizes individual competences, is inspired by mutual trust and loyalty and is based on the respect for everyone's personality and dignity.

Professional competences and proper conduct of staff members are the key assets of the Bank and contribute to its efficiency and competitiveness.

Human resources management policy

MB Lux valorizes its staff on a meritocratic basis, developing its professional skills in accordance with the principle of equal opportunities and in accordance with its own strategic choices, organizational and productive requirements, taking into account also its staff members' training needs.

Professional development is ensured also through adequate education initiatives, working experiences guided by line managers, possible transfers to different positions, performance assessment and career advancement.

The Bank recognizes the strategic role and central position of professional development and promotes training on an ongoing basis with initiatives consistent with the duties performed and with the staff's level of preparation and experience.

Staff selection and recruitment process is based on objective skills and professionalism requirements, taking into account specific organizational requirements and ensuring equal opportunities in terms of employment and professional development on a meritocratic basis.

Managers are required to make growth of their staff a priority, and to create an inclusive work environment, to attract and retain the best individuals and allow the team to innovate, solve problems and perform at its best.

Equal opportunities, discrimination, harassment and mobbing

Mutual respect is the basis for building trust and cooperation. Therefore, the Bank avoids every form of discrimination or harassment based on age, gender, sexual orientation, civil status, religion, language, ethnic of national origin, state of health, physical or mental disability, pregnancy, maternity or paternity (including by adoption), personal convictions, political opinions, affiliations or activities.

Diversity is a significant asset that expands cultural horizons and enables the Bank to provide improved services to its clients. Achieving excellence requires an inclusive environment which welcomes and supports differences and encourages a plurality of viewpoints.
Heads of units and offices shall promote a climate of open communication, mutual trust and collaboration.

The Bank forbids any unwanted behavior expressed in physical, verbal or non-verbal form, the purpose or effect of which is to violate the dignity and liberty of an employee and to create an intimidating, hostile, degrading, humiliating and offensive environment.

Recipients who suffer or are present at instances of discrimination, harassment or mobbing must report them promptly to the Group Human Resources. Such reports will be managed

with confidentiality and ensuring there are no retaliation or discrimination against the parties involved.

Q. I overheard my colleague refer to another colleague using a racist term. What should I do?
A. The Bank does not tolerate any form of discrimination; hence any person who is present when an instance of discriminatory behavior takes place must report the fact promptly to the Group Human Resources.

Grievance and internal complaints

The Bank promotes open communication and invites the Recipients to solve any difficulty they encounter in the workplace with the person directly involved or their line manager through informal meeting. If this approach does not lead to a satisfactory solution, a dedicated process for grievance has been set up with the involvement of the Group Human Resources.

Health and safety in the workplace

MB Lux, aware of the importance of health and safety, guarantees an adequate working environment, implementing the necessary precautionary action to preserve the health, security and safety of the Recipients and the third parties who visit the Bank's offices.

MB Lux further provides the necessary tools for healthcare and assistance with in-depth check-ups and adequate information on oncological diseases.

The Recipients shall comply scrupulously with the prevention and security measures adopted, taking part in the training courses organized by the Bank on this topic.

Leaving Mediobanca International

The Recipients must comply with certain obligations and restrictions also after their professional or working relationship with MB Lux has ended.

In particular, the Recipients are bound to:

- return all company assets in their possession;
- maintain the privacy on the confidential information in their possession to the extent allowed under applicable regulations;
- refrain from dealing in financial instruments if they have inside information on the issuers;

- co-operate with any legal dispute, request or enquiry made by the Authorities on issue related to their working or professional activity with MB Lux.

14. Dealing with suppliers

MB Lux relies on suppliers that share the Bank's principles of proper conduct, transparency and collaboration, with a view to developing synergic and efficient relationships inspired by proper conduct, transparency and co-operation.

Suppliers selection and management

Recipients shall not influence unduly the supplier selection process, which is based on professional skills, economic and organizational resilience and stability and best value for money. Recipients shall keep agreements with suppliers and terms thereof confidential and shall not exploit this information for their personal benefit.

Suppliers are informed of the contents of the Code of Conduct and the obligation to comply with it. Accordingly, the Recipients who entertain relations with suppliers which breach the rules contained in the Code of Conduct undertake to activate all contractual and legal provisions to protect the Bank's reputation and rights, which may also include ending the relationship with the supplier.

Q. I have become aware through press articles that a key supplier of the Bank may be involved in money laundering. What should I do?
A. You should report it immediately to the Management, which will take appropriate measures.

Industrial and intellectual property protection

Recipients shall comply with the external regulations and contractual agreements with suppliers in terms of industrial and intellectual property.
In particular, the Recipients must not:

- Use IT programs without a proper license;
- Acquire or disseminate goods or works in a way that breaches industrial and intellectual property regulations.

15. Relevant internal regulations

- Group Sustainability Policy;
- Group Policy on Transparency in relations with Clients;
- Group IT risk management Policy;
- Group Directive on abusive behaviour, bullying and harassment;
- Group Directive on media relations, speaking policy, marketing and social media channels;
- Group Directive on the use of corporate assets;
- Code of Ethics;
- Whistle-blowing Policy;
- Policy for managing risk of non-compliance with regulations;
- Policy for managing Money Laundering and Terrorist Financing risk;
- Product Governance Policy;
- Personal data protection Policy;
- Policy for the management of conflicts of interest;
- Gifts Directive;
- Directive on transfers and expense refund claims;
- Compliance Breaches Directive;
- Directive on Dealing with the Public Administration;
- Regulations governing use of confidential and inside information;
- Regulation governing Personal Transactions involving Financial Instruments;
- Regulations on Internal Dealing;
- Policy for managing the risk of money-laundering and terrorist financing.
- Anti-Bribery & Corruption Directive;
- Policy on Business Conduct and related risks;
- Complaints handling Policy;
- Outside Business Interest Directive;
- AML Manual;
- Remuneration Policy;
- Group ESG Policy;
- Group Directive Business Continuity Management;
- Regulation for transactions with related parties and their associates;
- Group Directive information classification and management;
- Group Information Security Policy;

- Data Breach Policy;
- Group Procurement Process Management Directive.