

CODE OF CONDUCT

DECEMBER 2023

c^oface
FOR TRADE

SUMMARY

MESSAGE FROM THE CEO

3

1. OUR VALUES

4

2. OUR RESPONSIBILITIES

6

COFACE EMPLOYEES

COFACE MANAGER

PENALTIES FOR MISCONDUCT

RAISING A WHISTLEBLOWING ALERT

3. COMPLIANCE PRINCIPLES

14

FINANCIAL CRIME

- Money laundering
- International sanctions
- Fraud
- Bribery

CLIENT &
DATA PROTECTION

- Customers' protection
- Data privacy & data protection
- IT Security
- Security & business continuity

PROFESSIONNAL
ETHICS

- Conflict of interest
- Supplier relationships

MARKETS

- Insider trading
- Market rules

MESSAGE FROM CEO

Coface has successfully been doing business for 75 years and is now present in over 100 countries. The world is evolving at a rapid pace and we have to comply, in the multiple markets in which we operate, to more demanding regulations and to increasing expectations from our clients, employees, shareholders and the general public.

We can succeed together through our commitment and the respect of our values: Client Focus, Expertise, Collaboration, Courage & Accountability and at the bedrock of all, Integrity.

Whatever our activities or positions, it is not only our actions, but also how we behave, that ensure we remain exemplary. Yet, this is not always obvious in our worldwide activities, which are complex and highly regulated.

This Code of Conduct gives an array of simple, but critical, principles to guide each of us in our daily responsibilities. It provides advice to identify situations that might cross the line, and guidance on how to address such situations.

It is essential that each employee knows, understands and applies the rules and principles of this Code. Managers must ensure that it is respected and set the example to protect the quality of our business relationships in all our operations and markets.

I thank you for your commitment and vigilance to protect our integrity, which is essential for our Group's successful and sustainable growth.



XAVIER DURAND



1. OUR VALUES

OUR VALUES

COFACE IS COMMITTED TO OPERATING ETHICALLY AND RESPONSIBLY IN ALL OF ITS BUSINESSES THROUGHOUT THE WORLD. OUR VALUES GUIDE OUR BUSINESS' OPERATING PRINCIPLES AND THE BEHAVIOURS OF EACH OF OUR EMPLOYEES.

CLIENT FOCUS

We are a client-centric company. Our customers and partners are our top priority. We put client satisfaction at the centre of our business. We offer products and services adapted to client needs because we stay connected to the market, we understand macro-economic trends, competitor moves, and because we know how to listen carefully and to be flexible. In this way, we build and maintain strong and durable relationships with our clients, brokers and partners.

COLLABORATION

We work in the spirit of 'one Coface' - cooperating across functions, departments and countries, informing and helping our colleagues to deliver to our clients and partners around the world. We are transparent and behave with integrity in our professional relations. We value everyone's contribution and take time to celebrate our successes. We foster sharing and support throughout our network of entities and external partners to better leverage our wealth of experience and achieve outstanding performance.

EXPERTISE

We continuously strive for excellence in all our fields of expertise: quality information and underwriting, in-depth knowledge of our markets and sectors, first-class economic research... To do so, we are committed to strengthening our leadership and people management. This is how we ensure we keep ahead of risk trends and propose the optimum solutions to facilitate and develop our clients' businesses.

COURAGE & ACCOUNTABILITY

We are empowered and take ownership for our decisions, our actions and their consequences. We proactively communicate and explain the basis of our underwriting and commercial decisions to clients and partners within the limits of our confidentiality obligations. We strike the right balance between growth and risk. Our delegation and reporting processes are transparent, our strategic and budget processes participative. We embrace new ideas and pioneer and test innovation across our business to better serve our clients.



INTEGRITY

Integrity is the bedrock on which our corporate values are built. Throughout Coface we abide by the highest standards of ethics and professional conduct. We are honest, sincere and transparent in all our dealings and 100% compliant with both internal Group rules and the regulations that govern our business in the markets where we operate.



2. OUR RESPONSIBILITIES

THE DUTIES OF ALL COFACE EMPLOYEES

ALL EMPLOYEES MUST CONTRIBUTE TO COFACE'S COMPLIANCE CULTURE BY UNDERSTANDING ITS POLICIES, EMBRACING ITS COMMITMENT TO INTEGRITY AND ACTING TO ENFORCE COMPLIANCE AND AVOID VIOLATIONS.

UNDERSTAND AND COMPLY WITH COFACE POLICIES

- Gain basic understanding of the policy requirements summarised in the Code of Conduct.
- Learn the details of the policies relevant to your job.
- Check WeConnect for the complete and up-to-date Group policies.
- Follow local policies and procedures in addition to those described in the Code of Conduct.
- Ask any questions about the policies to your manager or Compliance Officer.

REPORT COMPLIANCE ISSUES OR CONCERNs

- Promptly raise any concerns about potential violations of a policy.
- Know the different channels for the raising of integrity alerts: your manager, your Human Resources Manager, your Compliance Manager, as well as the channels specific to integrity concerns including the Ombudsperson and channels accessible to the public via the Coface website (form or generic email address).
- Cooperate in investigations related to integrity concerns.

ACT TO PREVENT COMPLIANCE ISSUES IF APPROPRIATE

- Be knowledgeable about and comply with the Coface policies that affect your job responsibilities.
- Be aware of the specific regulatory requirements of the country where you work and that affect your business.
- Promptly report any red flags or potential issues that may lead to a regulatory compliance breach.
- Always treat regulators professionally, with courtesy and respect.
- Ensure that you coordinate with business and support functions when working with or responding to requests of regulators.

WORKING ENVIRONMENT

- Employees must be able to work in a positive environment that promotes safety and reflects the values of respect and collaboration towards colleagues, subordinates, managers, customers, suppliers and third parties with whom we interact.

EXEMPLARITY OF MANAGERS

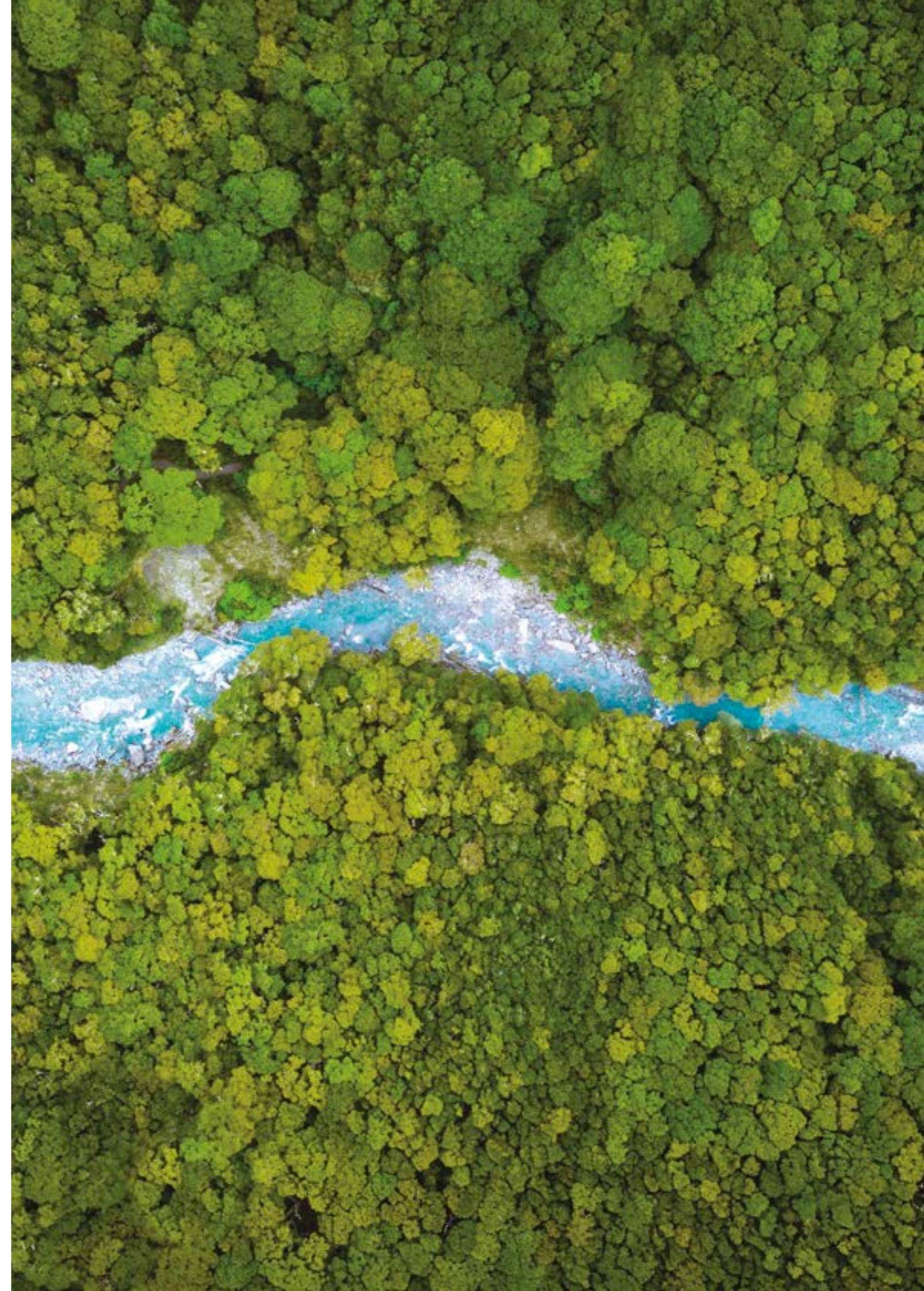
- Managers must be exemplary in the way they carry out their supervisory responsibilities.
- They must ensure that their behaviour is not perceived as harassing or intimidating, and that everyone in their teams is treated with respect and dignity by any other team member.
- In relation with work, managers must pay a particular attention to the well-being and the mental health of the employees they are responsible for.

RESPECT FOR PRIVACY

- Employees must respect the privacy and personal data of everyone, in accordance with the regulations applicable in their country.

NON-DISCRIMINATION, DIVERSITY, EQUITY AND INCLUSION PRINCIPLES

- Employees must ensure a working environment free of discrimination of any kind, whether based on age, gender, sexual orientation, culture or nationality, religion, health, disability or any other difference.
- These principles must be particularly followed during recruitment, hiring, training, evaluation, salary reviews and promotion, which must be based exclusively on merit, skills and individual performance.
- Beyond the principles of non-discrimination above, employees should be promoters of an inclusive environment, where everyone should feel valued for what they are, regardless of any differences.
- Coface has defined a diverse, equitable and inclusive policy that specifies our commitments in this area.



THE DUTIES OF ALL COFACE MANAGERS

IN ADDITION TO THEIR RESPONSIBILITIES AS EMPLOYEES, MANAGERS ALSO HAVE THE DUTY TO BUILD AN ENVIRONMENT TO PREVENT, DETECT AND RESPOND TO COMPLIANCE ISSUES.

SUSTAIN A CULTURE OF COMPLIANCE

- Create a culture of compliance in which employees understand their responsibilities and feel comfortable raising concerns without fear of retaliation.
- Encourage ethical conduct and compliance with the law by actively supporting compliance efforts.
- Consider compliance efforts when evaluating and rewarding employees.
- Ensure training on Coface policies and applicable law is provided to employees and (where appropriate) third parties.

PREVENT COMPLIANCE ISSUES

- Identify business compliance risks.
- Ensure that processes, tailored to address your particular risk areas, are communicated with all employees and implemented effectively.
- Allocate the necessary resources to the business's compliance program.

DETECT COMPLIANCE ISSUES

- Implement permanent control measures to detect heightened compliance risks and/or violations.
- Promote an effective ombudsperson system.
- Ensure that periodic compliance reviews are conducted, with the assistance of business compliance leaders and/or the internal audit.

RESPOND TO THE COMPLIANCE ISSUES

- Contact Compliance department and take promptly the necessary measures to fix identified compliance weaknesses.
- Take appropriate disciplinary actions if necessary.
- Notify the supervisory authorities, in collaboration with the Compliance department, if necessary.



LEAD

- Ensure that you and your team are engaged in complying with policies, meeting regulatory requirements and managing related risks.
- Integrate regulatory requirements into operational processes.

ASSESS

- Determine the key regulators and regulatory requirements that affect your business operations globally.

RESOURCE

- Assign owners for all regulatory risk areas and ensure that they coordinate with any relevant authorities.
- Liaise with the relevant team to effectively manage regulatory and compliance matters.

ANTICIPATE

- Implement effective regulatory watch.
- Include relevant regulations in your risk assessments.

RELATE

- Develop and maintain effective relationships with relevant authorities in coordination with Compliance.
- Work proactively with regulators on the development of regulations that achieve policy objectives efficiently and effectively.

CONTROL

- Assure the corrective actions on recommendations issued by regulators and internal auditors are closely monitored and effectively implemented.

PENALTIES FOR MISCONDUCT

EMPLOYEES AND MANAGERS WHO VIOLATE COFACE'S POLICIES ARE SUBJECT TO DISCIPLINARY ACTION THAT MIGHT RESULT IN TERMINATION OF EMPLOYMENT.

MISCONDUCT THAT MAY RESULT IN DISCIPLINARY SANCTIONS INCLUDES:

- Violating law and regulation.
- Violating a Coface policy.
- Requesting others to violate a Coface policy.
- Failure to promptly raise a known or suspected violation of a Coface policy or an internal instruction.
- Failure to cooperate in Coface investigations of possible policy violations.
- Retaliation against an employee for raising a whistleblowing.
- Failure to take prompt corrective action to fix identified breaches of compliance with Coface policies, laws and regulations.



RAISING A WHISTLEBLOWING ALERT

IF YOU ARE AWARE, DIRECTLY OR NOT, OF A PRESUMED OR SUSPECTED INCIDENT ABOUT A BREACH OF THE LAW, OF THE COFACE CODE OF CONDUCT OR A THREAT TO THE GENERAL INTEREST, YOU HAVE A RESPONSIBILITY TO RAISE A WHISTLEBLOWING ALERT THROUGH THE WHISTLEBLOWING CHANNELS AS DEFINED IN THE GROUP WHISTLEBLOWING PROCEDURE.

WHY RAISING AN ALERT?

- You should raise an alert early: the longer we wait to address the situation, the worse it may become.
- Raising an alert protects Coface, its employees and stakeholders.
- All alerts are received, escalated, processed and archived in an impartial and confidential manner. Each situation is handled without bias, in complete objectivity and your identity is treated in confidence, from the whistleblowing receiving to the end of the data retention period.
- Retaliation violates Coface policy: Coface absolutely prohibits retaliation against anyone for raising an alert in good faith. Retaliation is grounds for disciplinary sanctions up to and including dismissal.

WHAT HAPPENS WHEN AN ALERT IS RAISED

Presumed or suspected incident about a breach of the law, of the Coface Code of Conduct or a threat to the general interest will be investigated, as per the following process:

- The appropriate team/function to conduct future investigations is designated by the Whistleblowing Forum or the Ombudsperson, depending on the first channel contacted by the whistleblower.
- The specifically designated team/function then conducts investigations and determines the veracity of the alleged facts through interviews and/or review of documents. The conclusions are presented to the Whistleblowing Forum or the Ombudsperson.

- When the case is proven right, all necessary remediation measures are taken to put an end to the situation reported and/or to ensure that the situation will not happen again. Adequate follow-up is performed.
- Throughout the management of its alert, the whistleblower has right to information and receives an acknowledgement of receipt, proper feedback and notification of closure on the outcome.

HOW TO RAISE AN ALERT

- You can raise an alert verbally or in writing.
- An alert can also be raised anonymously. However, you are not encouraged to do so, in order for the investigations to be properly conducted. Also, Coface is strongly committed to protect those who raise an alert in good faith. If you identify yourself, we are able to follow-up with you and provide feedback.
- As described in the Group whistleblowing procedure, several channels are available for raising an alert. Use the channel that is most appropriate for you.
- Within your business, you may turn to:
 - Your designated HR manager;
 - Your designated Compliance officer.
- Other possible channels:
 - The Coface Ombudsperson at the following address : ombuds@coface.com;
 - The online form accessible on the Coface public website;
 - The generic mail address: whistleblowing@coface.com

3. COMPLIANCE PRINCIPLES

4 QUESTIONS TO ASK ONESELF

1. Are my actions **legal**?
2. How would the decision be **perceived** by others?
3. Am I prepared to be **accountable** for the decision?
4. Is it consistent with Coface's **Code of conduct**?

4 RESPONSIBILITIES

1. **Be** honest, sincere, transparent and fair.
2. **Comply** with applicable laws and regulations.
3. **Report** any compliance issue or concern.
4. **Act** to prevent compliance issue if appropriate.

FINANCIAL CRIME

Anti-money laundering

RULES TO REMEMBER

FOLLOW THE “CUSTOMER DUE DILIGENCE” (CDD) PROCEDURE; REPORT YOUR CONCERN IF YOU IDENTIFY SUSPICIOUS ACTIVITY.



WHAT TO KNOW

- Coface is committed to complying fully with all anti-money laundering and anti-terrorism laws throughout the world. Coface will conduct business only with reputable customers involved in legitimate business activities, with funds from legitimate sources.
- People involved in criminal activities, such as terrorism, narcotics, bribery or fraud, may try to “launder” the proceeds of their crimes to hide them or make them appear legitimate.
- Most countries where Coface operates now have laws against money laundering, which prohibit conducting transactions that involve proceeds of criminal activities.

- A related concern is that legitimate funds may be used to finance terrorist activity — sometimes called “reverse” money laundering.
- Each Coface entity is required to comply with the «Customer Due Diligence» procedure and to take reasonable steps to prevent and detect suspicious operations.
- Failure to detect customer relationships and transactions that put Coface at risk can severely damage Coface’s integrity and reputation.
- Keep in mind that Customer Due Diligence is not limited to an administrative process but requires an analysis of all information collected.



WHAT TO DO

- Comply with all applicable laws and regulations that prohibit money laundering and terrorism financing.
- Understand how these laws and regulations apply to your business.
- Follow your business’ rules concerning acceptable forms of payment. Be vigilant concerning the types of payments that have become associated with money laundering (for example, multiple money orders, cash, wire transfers or cheques on behalf of a customer from an unknown third party).

- Become familiar with red flags associated with money-laundering.
- If you notice a warning sign of suspicious activity, raise your concern to your Compliance Officer and be sure to resolve your concern promptly before proceeding further with the operation. Ensure the resolution is well documented and that all suspicions are kept strictly confidential (“tipping off”).



WHAT TO WATCH OUT FOR

- A customer, agent or proposed business partner who is reluctant to provide complete information, provides insufficient, false or suspicious information, or is anxious to avoid record keeping or reporting requirements.
- Payments using monetary instruments that appear to have no identifiable link to the customer or have been identified as money laundering mechanisms.
- Attempts by a customer or business partner to pay in cash.
- Orders, purchases or payments that are unusual or inconsistent with the customer’s trade or business.
- Unusually complex deal structures, payment patterns that reflect no real business purpose, or unusually favourable payment terms.
- Unusual fund transfers to or from countries unrelated to the transaction or to the customer.
- Operations involving locations identified as risky such as tax havens or areas of known terrorist activity, narcotics trafficking or money laundering activity.
- Operations involving foreign shell or offshore banks or nonbank financial intermediaries.
- Structuring of operations to evade record keeping or reporting requirements (for example, multiple transactions below the reportable threshold amounts).
- Requests to refund or pay claims to an unrelated third party or unknown or unrecognized account.



IN PRACTICE

A new policyholder wishes to pay for their policy in cash. Can you accept it?

You have doubts about the legality of the operations of a specific client. What should you do?

The economic capacity of a client is not consistent with the exposure policy. Should this be a cause of concern?

You are about to pay a claim and the policyholder asks you to pay the claim to a different bank account. Do you pay the claim to that account on the basis that the details were given by the policyholder?

A client paid a premium in Hong Kong dollars, but requests claims payment in U.S dollar without a legitimate reason. What do you do?

› No, under no circumstances should you accept cash. You must inform the Compliance Officer immediately of the offer.

› If you detect that a prospect or a client, its shareholders or executives, have been linked to unethical conducts, criminal activities or have negative reputational information, you must inform your local Compliance Officer.

› This should alert you because the income from illegal activities could be hidden. Any unusual or atypical situations should be considered a red flag and the Compliance Department must be notified.

› We can only pay a claim to an account bearing the name of the policyholder or that of a designated loss payee. Paying a claim to a third party would be tantamount to laundering money.

› You should inform your Compliance Officer about this suspicious activity.

International sanctions

RULES TO REMEMBER

ENSURE THAT ALL COUNTERPARTIES, THE UNDERLYING TRANSACTIONS AS WELL AS THE COUNTRIES INVOLVED ARE NOT SUBJECT TO INTERNATIONAL SANCTIONS.



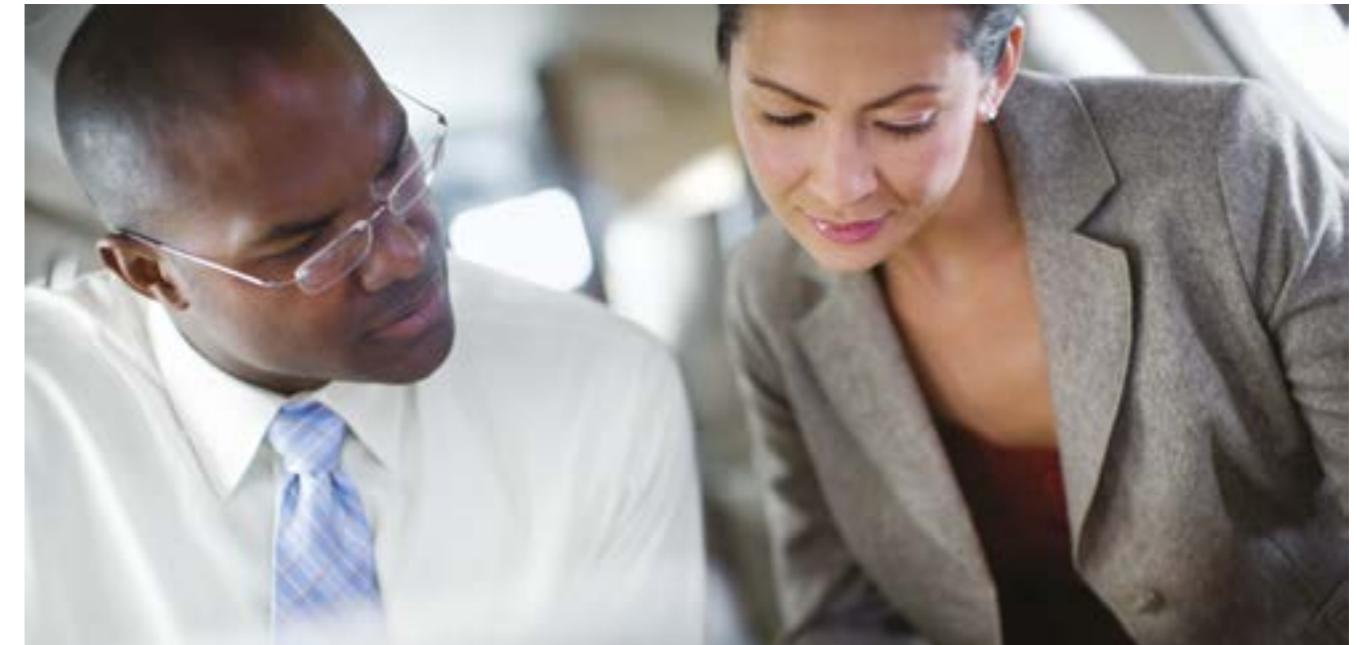
WHAT TO KNOW

- As part of its Global Sanctions policy, Coface complies with resolutions issued by the United Nations Security Council (UN) as well as laws and regulations from European Union (EU), France and the Office of Foreign Assets Control (OFAC) of the United States Department of the Treasury.
- In addition, Coface observes any additional local sanctions laws and regulations in countries where it operates.
- Coface prohibits coverage of any operation involving, directly or indirectly, individuals or entities (including customers, suppliers, distributors, other counterparties, agents or employees) subject to asset freeze measures as imposed by the UN, EU, French, OFAC or other relevant local sanctions lists.
- Coface does not cover the sale of goods that do not comply with international sanctions.



WHAT TO DO

- Follow the regulation and procedures applicable in all countries where you operate.
- Check the underlying transaction and ensure that it does not involve countries, persons, goods or activities subject to international sanctions.
- Screen all the parties involved in your operation (business partners, suppliers, intermediaries, third parties, etc.).
- Follow the «Customer Due Diligence», the International Sanctions and the Dual-use goods procedures.
- Do not engage in any restrictive trade practice that is prohibited under Coface Rules and Policies or applicable local laws.
- Consult your manager if an operation involves a conflict between Coface Policies and applicable local laws (e.g. laws adopted by Canada, Mexico and the members of the European Union blocking certain U.S. restrictions).



WHAT TO WATCH OUT FOR

- Any elements that suggest your customer may be attempting to evade sanctions.
- Evasive, reluctant or otherwise unsatisfactory answers by a customer to questions on the underlying transaction about end use, end user, delivery dates or delivery locations.
- Involvement of parties or activities suspected of any connection with the development of biological, chemical or nuclear weapons, or ballistic missiles.
- Operations involving an individual or an entity subject to sanctions or a country under embargo.
- Policies with incomplete information on the underlying operation (e.g. price shown does not reflect the full value, the description of the goods is not complete, or the country of origin is not correctly identified).



IN PRACTICE

Company A, registered in BVI, offers shipping services worldwide. While conducting a KYC periodical review, you discover that one of their vessels is subject to sanctions because of its involvement in the sale of Russian oil in violation of international sanctions? What do you do?

› You should inform your Compliance Officer immediately.

Fraud

RULES TO REMEMBER

BE AWARE OF INCONSISTENCIES; FOLLOW CONTROL PROCEDURES, KYC AND SEGREGATION OF DUTIES; REPORT SUSPICIOUS CASES.



WHAT TO KNOW

- The responsibility for the prevention, identification and reporting of fraud is both a corporate and an individual responsibility.
- Coface and its employees are required to demonstrate diligence and report matters promptly. When employees act in good faith and promptly report a potential suspicious or fraudulent incident, it lowers the risks of legal proceedings and financial loss.



WHAT TO DO

- Follow the "Customer Due Diligence", "Know Your Intermediary" and "Know Your Supplier" procedures.
- Understand the business purposes for which Coface's products and services are used.
- Respect segregation of duties, especially for payments.
- Protect Coface assets from theft or misappropriation.
- Make a counter-call to your customer, partner, supplier, using a known and verified contact (phone number, email address etc.) before making a payment to a new bank account.
- Make sure you have a genuine invoice, validated for each payment.
- Report any suspected fraud case; contact your manager or entity fraud correspondent.



WHAT TO WATCH OUT FOR

- A policyholder who adds or increases insurance shortly before submitting a claim.
- Very urgent request, order concluded without price negotiations.
- Many requests in a short period of time.
- Numerous insistent telephone calls from the buyer, spontaneous sending of information by the buyer.
- The order includes only a mobile number and email addresses from free providers like Yahoo, Gmail, and Hotmail.
- Products sold are inconsistent with activity of the insured or the buyer.
- The invoice and delivery addresses are inconsistent, and there is no confirmation of the delivery address in our records.
- Unusual documentation.
- Ghost companies: in such case, policies are issued and premiums accepted from policyholders, but the customer isn't legitimate and often doesn't exist.



IN PRACTICE

A newly created company requests a credit limit of several millions on a very well-known company. Although the order is worth several times the current turnover of the prospect, the contact is very vague when asked for details and is untroubled when Coface's checks confirm that the order is fake. Once the large credit limit is excluded, can you sign a policy with this prospect?

Company A and B were both set up 2 years ago, Company A has been Coface client since its establishment. Last month, Company A requested a significantly larger amount of coverage on Company B. Based upon the previous payment and credit history, significant coverage is provided. 3 months later, Company A informed Coface that Company B did not pay and went into bankruptcy. Company A submitted a claim which includes all of the documents such as the commercial invoice, packing slip, certificate of insurance, inspection certificate, bill of landing, etc., clearly demonstrating that the goods were shipped all in accordance with the terms and conditions of the contract.

Whilst it is difficult to know whether the prospect is a victim or not, the prospect has demonstrated that they are either not making basic checks or that what they say may not be trustworthy. A Coface policy might be used as a "badge of respectability" to defraud a funding institution or to launder money.

The Claims Department should conduct further investigation because there might be an insurance fraud as Company A might export fake goods from a country where shipping procedures are not strictly respected and the seller could easily create false documentation showing that goods were sent, when in fact no, or fake goods were shipped.

Bribery

RULES TO REMEMBER

DO NOT OFFER/ACCEPT GIFTS OR BENEFITS THAT COULD UNDULY INFLUENCE SOMEONE'S DECISION; MONITOR YOUR CLIENTS, BROKERS, SUPPLIERS AND ANY OTHER COUNTERPARTIES; REPORT ANY SUSPICIOUS ACTIVITY.



WHAT TO KNOW

- Coface has zero tolerance to bribery. Bribery is the offer, promise or giving (active bribery) or the soliciting, requesting or receipt (passive bribery) of an undue benefit to/ from a person in order to perform or not perform an action in the execution of their professional duties.
- The beneficiary can be either a public official or an employee of the private sector. It can also be a close relative of that person (such as a family member) or an associated entity, for example a foundation or a shell company.
- An undue benefit could be cash and cash-equivalent, but also anything of value including goods and services, gifts, trips, entertainment, hospitality, a promotion or an honour, the awarding of a contract or an official permit or an administrative decision.
- The undue benefit could be direct (e.g. bribe, undue commission, facilitation payment, lavish gifts or advantages, over-invoicing) or indirect (e.g. donation to political parties, charities and sponsorship, hiring proposal).
- The use of influence (influence peddling), real or deemed, of a public person shall also be included in the scope of bribery.



WHAT TO DO

- Seek advice from your Compliance Officer in case of doubt.
- Never give or receive monetary payment in any form whatsoever (e.g. cash, cheque, bank transfer, gift certificates, vouchers) to or from a client, a supplier, an intermediary or any third counterparty.
- Never give or receive to or from any public official any gifts or benefits unless prior written consent by the Compliance Officer.
- Inform and consult your Compliance Officer if you receive a gift or benefit of:
 - 200 euros (or stricter local thresholds) or more within a three-month period timeframe
 - a cumulative value of 500 euros (or stricter local thresholds) or more within a three-month period timeframe.
- Authorised gifts must be delivered exclusively to a professional address.
- Before giving a gift, engaging in customer entertainment or reimbursing customer travel expenses, make sure you understand and comply with applicable legal requirements, the Gifts and Benefits Procedure, the Antibribery Code of Coface and the customer's own rules.
- When authorised, make sure you record accurately such expenditures to reflect the true nature of the transaction.
- Be aware not to create the appearance of an improper business courtesy.
- Never make facilitation payments, which means to pay directly or indirectly a public official unduly for the execution of administrative formalities which should be obtained by legal means.
- Never give political contributions on behalf of Coface. You can only address lobbyists if such lobbyists fully disclose that they represent Coface.
- You can sponsor a charitable organisation but must contact your competent compliance officer and ensure that the purpose of the supported entity is not to conceal bribery.



WHAT TO WATCH OUT FOR

- An amount of commissions unusually high or paid in an atypical way (e.g. separate account or jurisdiction).
- Significant over-billing under the contract without reasonable cause.
- Significant reductions on the premiums, commissions or price requested from the client without reasonable cause.
- Significant reductions on the price paid to a supplier or an intermediary without reasonable cause.
- Informal meetings with private and public companies for agreement on government procurement.
- Any request for a facilitation payment.



IN PRACTICE

A salesperson invites the same broker to lunch several times a month at relatively expensive restaurants and always pays the bill. In return, the broker favours Coface above any other credit insurer and sends a large number of enquiries. Is this bribery?

A supplier invites you to the final of a famous sporting activity and will bear all the travel costs. In parallel, they ask for an unusual high commission price in the transaction you are currently negotiating.

To increase your chances of acquiring a license in order to conduct insurance business in its country, the local insurance authority strongly encourages you to use a specific local consultant.

Whilst networking and nurturing relationships is part of a salesperson's job, entertaining and spending should be reasonable and proportionate. It could become bribery if the amount spent on entertaining one person is disproportionate to what is spent on other brokers.

The potential amount seems to be considerably higher than the 200 euro ceiling. This invitation from a supplier does not seem to meet the criteria of reasonableness and appropriateness to help establish, maintain and develop good relations between trading partners. The recommendation is to decline this invitation and inform your Compliance Officer.

The local consultant may have specific skills and knowledge that could improve the odds of successfully obtaining the license. But it could also expose Coface to be part of a bribery scheme of public officials, which is a criminal offence. You need to coordinate with the Group Legal Department, ensure that real work will be performed and that evidence of it is kept.

CLIENT & DATA PROTECTION

Customers' protection

RULES TO REMEMBER

**DO NOT SELL INAPPROPRIATE PRODUCTS TO CLIENTS;
ALWAYS ACT UNDER CUSTOMER MANDATE;
DO NOT OMIT TO PROVIDE INFORMATION LEGALLY DUE TO CLIENTS.**



WHAT TO KNOW

- Conduct of business risk can be described as “the risk to customers, insurers, the insurance sector or the insurance market that arises from insurers and/or intermediaries conducting their business in a way that does not ensure fair treatment of customers”.
- The entire product lifecycle is subject to different kinds of conduct issues: new products, sales, claims, client servicing.



WHAT TO DO

- Include conduct risk considerations into new product development.
- Ensure customer onboarding processes are correctly applied and respect customer complaints management procedure.
- Monitor product suitability at all client relationship stages.
- Train staff on insurance distribution.
- Integrate conduct risk considerations into sales incentive programs.
- Ensure that Coface and its partners are authorized to sell the product to the customer.
- Provide explanations in a timely manner to companies whenever a credit limit is modified or cancelled.
- Inform the policyholder of new relevant information about their insured customers, for example significant change in one of their debtors credit worthiness or of its solvency evolutions.



WHAT TO WATCH OUT FOR

- Products which do not represent a fair value for money.
- Sales processes do not match customer needs.
- Reward measures for commercials are unclear and not properly integrated into the remuneration frameworks.
- Intermediaries and brokers who have a weak compliance program and are not familiar with Coface's values and strategy.
- Complex claims process.
- High levels of customer dissatisfaction on the claims settlement process.
- Attempts to lower aggregate claims costs by not settling or delaying the settlement of valid claims.
- Insufficient explanation as for the reasons of the refusals.
- Barriers to complaints.



IN PRACTICE

You have a very tight deadline for launching a new product. You can gain time by skipping the review with the product committee and the Compliance Department, as it can be done after the product launch. What do you do?

- The product committee must be involved and the regulatory requirements taken into account before the product launch.

Data privacy & data protection

RULE TO REMEMBER RESPECT PRIVACY RIGHTS.

WHAT TO KNOW

- Most countries in which Coface operates have strict regulations on the collection and use of consumers' "personal data" (any data that can identify directly or indirectly an individual).
- In addition, many countries regulate personal data of company representatives in business-to-business transactions. A few countries

- even regulate the privacy of information relating to corporations.
- Coface is committed to handling personal and confidential data responsibly and in compliance with applicable laws and regulations relating to the protection of privacy and data security.

WHAT TO DO

- Learn and comply with the rules concerning personal data, notably:
 - Applicable laws and regulations of jurisdictions from which the personal data is collected and in which it is processed or used;
 - The privacy policies of Coface and your local business;
 - Any contractual obligations that apply.
- Collect, process, use and store relevant personal data for a legitimate purpose only.
- When possible, practice anonymisation, encryption or removal of personal or confidential information.
- Restrict the access to confidential or personal data to individuals who need it for a legitimate business purpose.
- Protect the confidential or personal data especially during remote work.

- Immediately notify your manager, your data privacy officer («DPO») or your Compliance officer if you learn:
 - that personal data has been used in violation of this policy; or
 - that the security of any system or device containing personal data has been compromised.
- Dot not consult confidential information in public transport.

WHAT TO WATCH OUT FOR

- Inadequate access or security controls such as e-mailing or otherwise distributing personal data to a larger group than legitimately needed, or leaving documents with personal data for others to see, notably at the printer machine.
- Sharing of personal or confidential data with third parties, such as vendors or suppliers, who lack appropriate security safeguards or restrictions on information use.
- Transfers of personal data between countries, without considering applicable legal requirements.

IN PRACTICE

You have signed a Non-Disclosure Agreement to obtain financials, is it acceptable to divulge the financial information to the policyholder?

You need to do some work at home that requires confidential information of a client. Can you send the client's information to your personal e-mail to continue working from home?

You are hiring the services of an external IT company that will give your company some essential services for your local operations. For providing the service, this external company will need to access to internal databases that might have information of our clients.

What should you do?

When meeting a customer, you become convinced that something is not right and you believe that the Financial Director is hiding something or is involved in suspicious activities. When you write the report, you are careful not to refer to the Financial Director by name so as to avoid data protection issues. Can the said person demand to see what is written on themselves in the report?

- No, under no circumstances should the information be divulged, the financials should also be saved as confidential.
- No, the clients information should always remain inside the company and personal e-mails accounts should never be used to transmit confidential information.
- You should avoid as much as possible sharing client information with third parties. If they really need to access our database, then you need to ensure that the contract with the external has adequate confidentiality clauses. These clauses should comply with the standards of the group on matter of Data Protection. In any case, such a contract should be reviewed by your Legal/Compliance Department.
- Data protection covers directors, employees and any identifiable person. If you state a person's position without writing their name, then that person becomes identifiable and is covered by data protection.



IT security

RULE TO REMEMBER

PROTECT COFACE INFORMATION, NETWORKS AND IT DEVICES AGAINST CYBER RISKS.



WHAT TO KNOW

- As a user, you are ultimately the last line of defence.
- Internet is a network that can be used for malicious purposes.
- USB devices may infect our IT system.
- Suspicious behaviors from your workstation may indicate suspect activity.
- Traditional and instant messaging platforms facilitate the act of pretending to be another individual.
- No Coface employee will ask for your credentials, and you must not disclose them.
- Use only the tools provided by Coface for storing or exchanging data.



WHAT TO DO

- Do not attempt to disable security features and apply instructions given, remotely or in Coface premises.
- Recognize phishing, be aware of attempts to improperly acquire Coface information or to act fraudulently. If in doubt, do not open an attachment, do not click on a link and alert the cybersecurity team without delay.
- Never disclose passwords; follow the password rules regarding complexity and renewal.
- Never use your Coface password on an external site; always choose a different password for each site.
- Only work on files on Coface servers to ensure they are properly saved.
- Be cautious online and do not persist in accessing sites that are blocked by Coface; avoid trying to visit them through alternative means.
- If you have any doubts, contact cybersecurity@coface.com



IN PRACTICE

Someone you know sends you an email with a link. You notice that the writing is different from their usual style, but you click on the link because you know the person well.

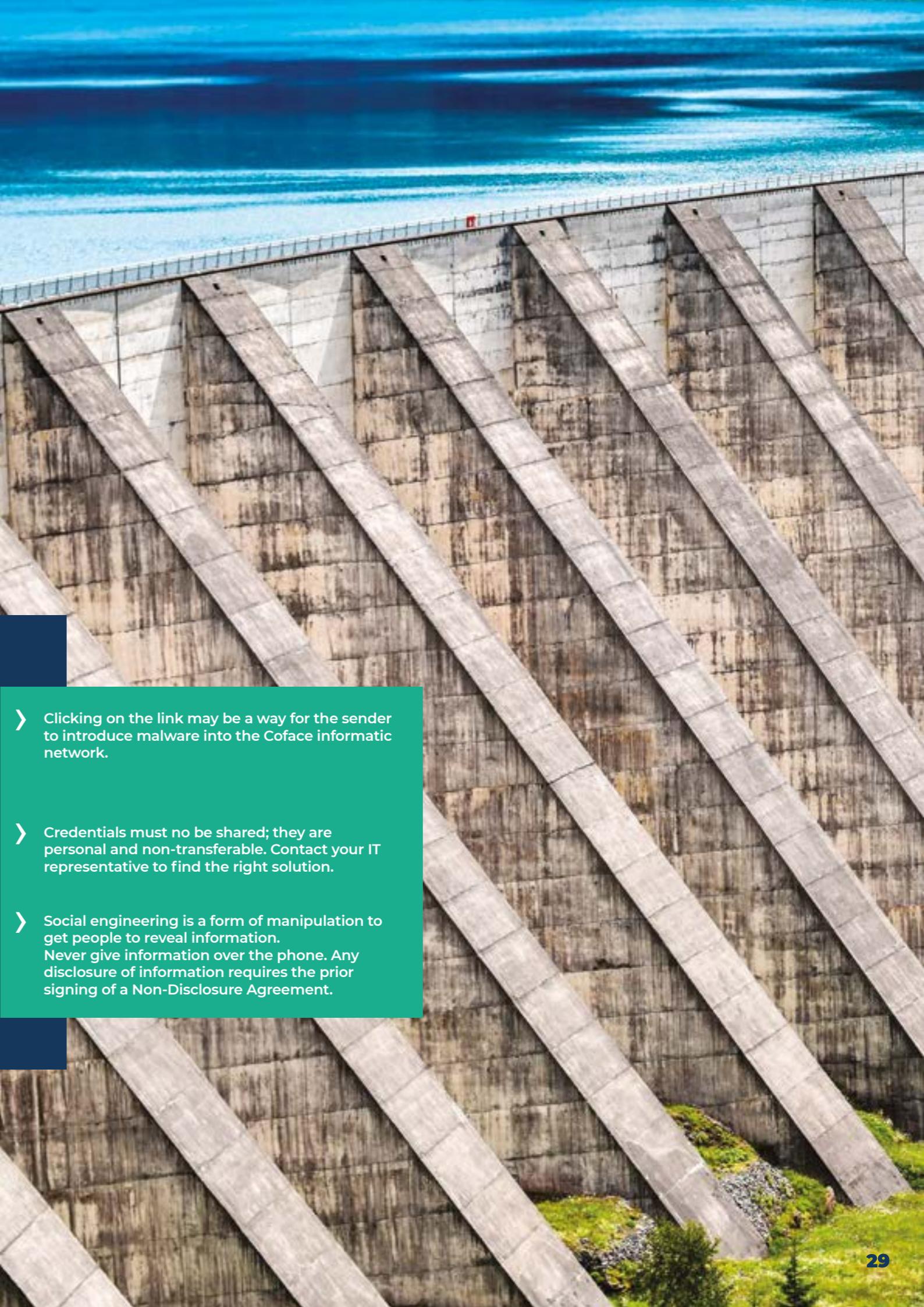
What should you do?

Your manager is very busy and asks you to log on to a tool or an application, using their login and password to retrieve some reports.

What do you do?

You received a phone call from a company proposing a new tool that could really help you in your daily tasks. You are then asked for very specific information about your computer, applications that you are already using...

What do you do?



Security & business continuity

RULE TO REMEMBER

ENSURE THE SECURITY OF EMPLOYEES, FACILITIES, INFORMATION, IT ASSETS AND BUSINESS.



WHAT TO KNOW

- Every Coface business entity implements a rigorous and comprehensive security and crisis management plan to protect the security of staff, workplaces, information and businesses.
- Coface's security and crisis management plan includes measures for preventing terrorism and other criminal acts covering the employees, facilities, information, information technology (IT) infrastructure, business continuity and crisis management.



WHAT TO DO

- Comply with the rules defined in the evacuation plan.
- Comply with the entry and exit rules at Coface facilities, including wearing the appropriate badge.
- Ensure that only authorized personnel can access Coface facilities.
- Protect Coface assets from theft or embezzlement.
- Identify and report any indicators of workplace violence.
- Conduct appropriate background checks on new hires and contractors, wherever allowed by law.
- Ensure that our key suppliers have business continuity plans to ensure the sustainability of their activities with Coface.
- Respect health and safety rules. Create and maintain a safe working environment with security and health protection for all employees.



WHAT TO WATCH OUT FOR

- Individuals at Coface facilities not wearing appropriate badges.
- Unsecure IT assets, such as laptops, servers, USB devices etc.
- Inadequate protection of hazardous materials.
- Unsecure areas of a facility where only authorised personnel are allowed to enter.
- Security complaints from employees, customers or neighbours.
- Unauthorised entry to a facility.
- Doing business with a customer, supplier or any third party without sufficient screening.



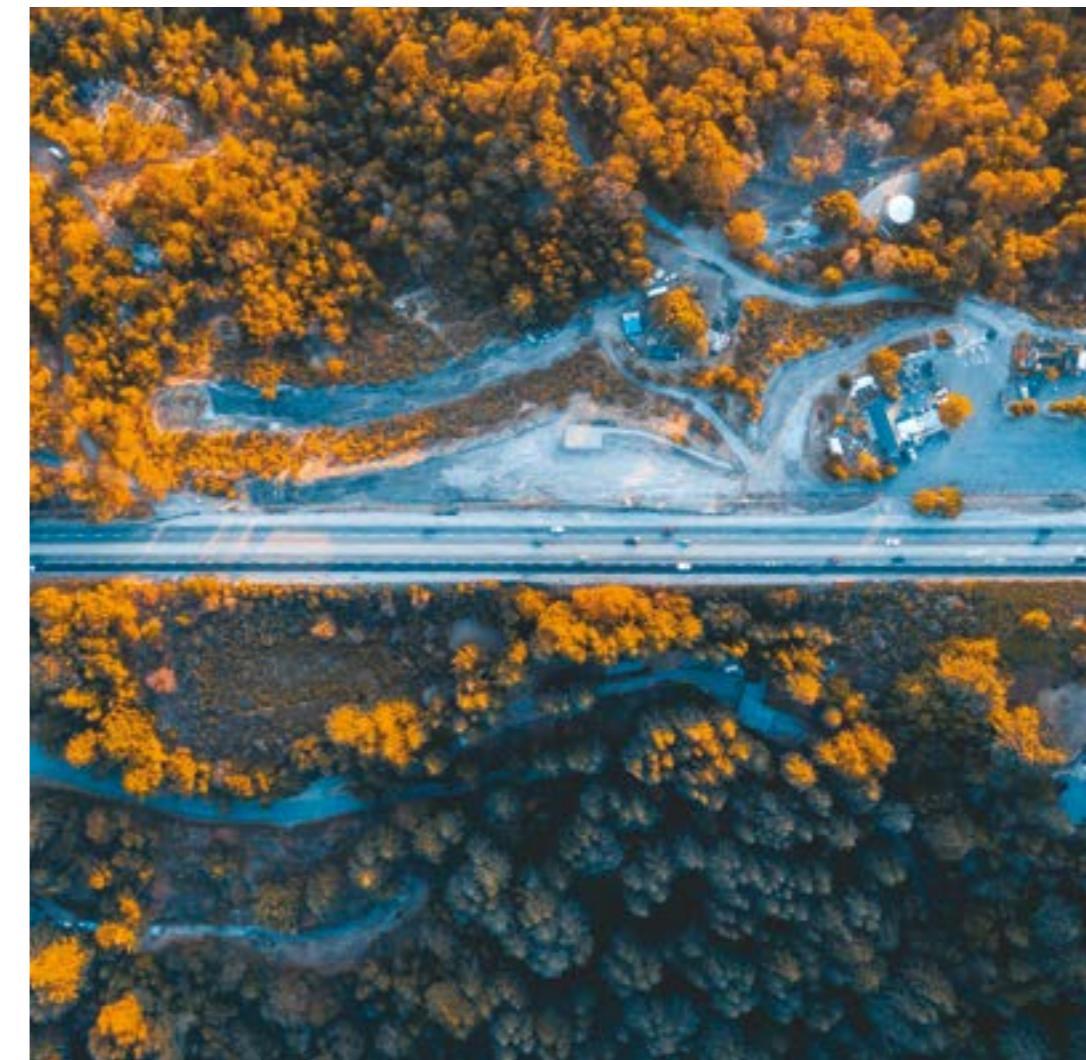
IN PRACTICE

Someone you do not know comes into the office and says that there has been a call for service by IT and they need to check something in the IT server room. Do you let them in?

A colleague stands at the entrance gate and asks you to let them enter the building using your access card. What do you do?

- Never ever let anyone work on any system unless you have been formally advised by your IT department that this person is coming and that it is ok to let them in.

- Direct the colleague to the security team or HR to obtain a substitute access card.



PROFESSIONAL ETHICS

Conflict of interest

RULES TO REMEMBER

DISCLOSE ACTIVITIES, INTEREST OR RELATIONSHIPS THAT COULD CONFLICT WITH YOUR RESPONSIBILITIES TO COFACE; DO NOT USE COFACE RESOURCES FOR PERSONAL GAIN.



WHAT TO KNOW

- Nothing you do, on the job or in your free time, should conflict with your responsibilities to Coface. No activity at work or at home should hurt Coface's reputation.
- Misusing Coface resources or influence is also prohibited.
- You need to consider how your actions might appear, and to avoid the perception of a conflict of interest. Even when nothing wrong is intended, the appearance of a conflict can have negative effects.



WHAT TO DO

- Disclose in writing to your manager and to your entity Compliance Officer all of your outside activities, financial interests or relationships that may present either - a conflict or - the appearance of one.
- Use good judgment in all personal and business dealings outside your Coface job.
- Avoid actions or relationships that may cause potential conflicts or create the appearance of a conflict with your job or Coface's interests.
- Do not use Coface resources, intellectual property, time or facilities for personal gain — this includes office equipment, e-mail and computer applications.
- Escalate any situation where a family member or a close relative has or may have a business relationship with a Coface competitor, partner, customer or supplier.
- Get Compliance approval before accepting officer or director positions with an outside business while you are a Coface employee, particularly if the organisation has a Coface relationship or might expect Coface financial or other support.



WHAT TO WATCH OUT FOR

- Financial interests in a company that might affect or appear to affect Coface's interest or the decisions taken (for example, a customer, supplier or investment).
- Part-time jobs, which you perform using Coface hours or Coface equipment or materials.
- Gifts of other than nominal value from suppliers, customers or competitors, particularly if you're making decisions (on Coface's behalf) that involve them.
- Personal discounts or other benefits from suppliers, service providers or customers of which you are the sole beneficiary.



IN PRACTICE

You are Commercial Underwriter and one of businesses that you are about to quote for is run by very good friend of yours.

Should you proceed with the quotation?

You work as a Key Broker Manager in Coface and a very close friend/relative has recently started working on a brokerage company that has a close business relation with Coface. This friend is actively involved in the credit insurance business.

What do you do?

You have started a relationship with an ex-Coface employee who now works for a competitor, and who has asked you for information on customers, pricing and underwriting. What do you do?

A client is asking for the approval of a very considerable credit line over a buyer with a bad record. The client invites you to a dinner and during it, he gives you tickets to your favourite band's concert. What do you do?

You work in the Risk Underwriting Department and one day, your uncle asks you for a favour. He would like to purchase insurance from Coface but thinks his company probably won't get the credit limit he wants and even if it does, the premium will be high. He would like you to "coach" him on how to fill the application and to prepare the documentation in order to get the credit limit he want at the lowest possible premium. What do you do?

- Granting contracts to suppliers related to your family members or close friends without prior information and approval to Coface.
- Misusing Coface resources, your position or influence to promote or assist an outside activity.
- Hiring, promoting or directly supervising a family member or close friend.
- Personal relationships that may conflict with your Coface responsibilities or compromise company interests.

› No. You must inform your manager and your compliance officer in order to appoint another team member to proceed with the quotation.

› A conflict of interest is not in itself a problem, but needs to be reported. In the example, you should report this relationship to your local Compliance Officer and they will analyse what measures could be taken to avoid any conflict of interest. Also you should avoid any situation/decision that could entail a conflict of interest.

› Sharing information with the competition might be a felony in your country and could be considered as a collusive conduct. Therefore, you should never share information with friends/relatives who are working for a competitor. Moreover, you should report this relationship to the Compliance Department.

› You should respectfully reject this gift. Receiving a gift of those characteristics could affect your objectivity for taking decisions. Moreover, you should report any gift that is not reasonable or too expensive (over 200 euros or stricter local threshold) to the local Compliance Officer.

› There is a conflict of interest and you should delegate the case to another team member. In the meantime, do not provide any help as it is unethical even with no reward involved.

Suppliers relationships

RULE TO REMEMBER

ENSURE COFACE WORKS ONLY WITH SUPPLIERS WHO COMPLY WITH LOCAL AND OTHER APPLICABLE LEGAL REQUIREMENTS AND COFACE GUIDELINES RELATING TO FINANCIAL CRIME, CLIENT AND DATA PROTECTION AS WELL AS LABOUR, ENVIRONMENT, HEALTH AND SAFETY.



WHAT TO KNOW

- Coface's relationships with suppliers are based on lawful, efficient and fair practices.
- Coface expects its suppliers to comply with the laws relating to financial crime, client and data protection as well as labour, environment, health and safety.



WHAT TO DO

- Comply with relevant regulations covering supplier relationships.
- Do business only with suppliers who comply with relevant regulations and Coface guidelines relating to financial crime, client and data protection as well as labour, environment, health and safety.
- Follow the procedures set out in Coface's procurement policy.
- Provide a competitive opportunity for suppliers to win contracts with Coface on open, competitive bidding.
- Protect Coface's confidential and proprietary information, as well as any information provided by suppliers with a non-disclosure agreement.
- Protect "personal data" obtained from suppliers.



WHAT TO WATCH OUT FOR

- Choosing suppliers on any basis other than open, competitive bidding.
- Potential conflicts of interest in supplier selection, such as accepting improper gifts or other items of value.
- Directing business to a supplier owned or managed by a relative or close friend without prior Compliance approval.



IN PRACTICE

You know a supplier who can provide a very competitive price for a product/service. Can you sign the contract directly with this company?

A supplier asks you to provide the HR data of Coface employees who will be using their services. Do you provide this information?

Your supplier offers very low prices, but you are uncomfortable with the working conditions of its employees. What do you do?

- Supplier who seems not to adhere to standards relating to financial crime, client and data protection as well as labour, environment, health and safety.
- Entrusting "personal data" or confidential information to suppliers without ensuring that they have appropriate technical, physical, and organizational measures to prevent unauthorised access or use.

- The Group Procurement Department must be involved when the value of the product/services exceeds the amount authorised in your country. Competitive tenders should be exercised, except for small amounts.
- Personal data is protected. You should consult with the Compliance Department before sharing any information.
- Coface's reputation and legal responsibility could be affected by suppliers who do not respect labour laws. You should report your concerns to your management.

MARKETS

Insider trading

RULES TO REMEMBER

**MAINTAIN THE CONFIDENTIALITY OF COFACE INFORMATION;
DO NOT BUY/SELL SHARES OF COFACE OR ANY COMPANY,
DIRECTLY OR INDIRECTLY, IF YOU KNOW INSIDE INFORMATION.**



WHAT TO KNOW

- Inside information is non-public information of a precise nature which, if disclosed, would reasonably be expected to affect the price of a security or would influence your decision to buy, sell or hold a security.
- Using non-public information of a precise nature for your financial or other personal benefit or conveying this information to others may constitute a violation of Coface policy and may violate the law.
- Inside information may be information about Coface or other companies that you learn in the course of your job. Inside information may also be a conversation you overhear or a memo left on a desk or at a copy machine.
- Unlawful use of inside information includes buying or selling the securities of Coface or any other company about which you have non-public information, but also giving this "inside information of a precise nature" to anyone else who might base financial trades on the information you've shared.



WHAT TO DO

- Do not buy or sell the securities of any company, including Coface, either directly or through family members or other persons or entities, while you are aware of inside information about the company (this is known as "insider trading") and especially 30 days before the yearly, half-yearly and quarterly financial results of the company are announced.
- Do not recommend or suggest to a third-party to buy or sell on the basis of inside information.
- Maintain the confidentiality of Coface information and do not convey information to anyone outside the Company unless it is necessary for the Company's business activities.
- Learn and follow the requirements relating to buying and selling securities (such as non-trade periods, pre-clearing personal trades,...)

if the nature of your business's activities or your position in the business subjects you to such rules.

- Notify, within 3 business days, the AMF and Coface of your transactions on Coface shares (purchase, sale, etc), when the total amount of transactions reach the threshold of 20,000 euros in one calendar year. This applies to people with managerial responsibilities those closely associated with them. When acquiring the shares of other French companies, the same thresholds apply, however for foreign companies make sure to comply with local regulations.
- If questions arise, consult your supervisor or Compliance Department or if you are a director of the company, the chairman of the board of directors before trading in the security or disclosing company information.



WHAT TO WATCH OUT FOR

- Non-public information of a precise nature which, if disclosed, would reasonably be expected to affect the price of a security or would influence your decision to buy, sell or hold a security (e.g. an earnings announcement).
- Buying or selling a security because you hear or learn of information at work that you think will make the price go up or down once it's publicly announced.
- Engaging in trading activity around the time of a significant company announcement.
- Discussing Coface business with family and friends.
- Talking about what you're working on or where you're going on company business or who visited the office.



IN PRACTICE

During a meeting with a client, they tell you that a company will merge with another which will probably increase the values of its shares on the market.
Can you buy some of these shares?

One day in the office, you overhear someone saying that Company X, one of our largest clients, has several customers, some of which who are not insured, who are defaulting on payment. These will cause some financial difficulties and the news will probably be announced in next week's stockholder meeting.

No, under no circumstances should you use insider-trading information to obtain a benefit on the financial market. In the example, you would have obtained information that was publicly not available and therefore, you would have had an unfair advantage over the rest of the market.

In many jurisdictions the use of insider trading information is strongly punished and is considered a felony.

You can't use this information to trade on Company X as you are using non-public material information.

Market rules

RULE TO REMEMBER

NEVER AGREE WITH COMPETITORS TO FIX PRICES OR ALLOCATE CUSTOMERS, PROJECTS OR TERRITORIES.



WHAT TO KNOW

- Competition and antitrust laws:
 - Prohibit agreements or understandings between competitors that undermine competition;
 - Regulate the behaviour of dominant companies; and
 - Require prior review and in some instances clearance for mergers, acquisitions and certain other transactions, in order to prevent transactions that would substantially reduce competition.



WHAT TO DO

- Comply with all applicable competition laws and regulations as well as competition law decrees, orders and agreements with any competition regulator about how business will be conducted.
- Comply and understand both Coface and business-specific policies and procedures, and if you have questions or issues, bring them up with company legal counsel.
- Do not propose or enter into agreements or understandings — expressed or implied, formal or informal, written or oral — with any competitor regarding any aspect of the competition between Coface and the competitor.
- Do not discuss with a competitor or competitor representative: Prices, bids, sales territories, allocation of customers or product lines, terms or conditions of sale, production, sales capacity or volume, costs, profits or profit margins, market share, product or service offerings, customer or supplier classification, distribution methods.

- These laws are complex, and global in reach, and can operate differently in any particular situation. Your business provides specific guidelines on addressing contacts with competitors, obtaining and handling data about competitors, and participating in trade, professional associations, standards setting and product certification organizations. In addition, it is often essential that you involve legal counsel early in the process of developing new commercial initiatives given the many uncertainties that arise in the application of these laws.

- Do not propose or enter into agreements with anyone (including competitors, agents, brokers or customers) regarding whether to submit a bid or the terms of a bid where there is an understanding that the bid is submitted for any purpose other than winning the business.
- Avoid contacts of any kind with competitors that could create the appearance of improper agreements or understandings.
- Do not propose or enter into agreements or understandings with customers that restrict the price or other terms at which the customer may resell or lease a product or service to a third party.
- Do not propose or enter into agreements or understandings with suppliers that restrict the price or other terms at which Coface may resell or lease any product or service.
- Consult with company legal counsel to help reduce the risks of noncompliance in the evaluation of any proposed merger, acquisition, joint venture or any other business arrangement that could raise competition law issues (examples of arrangements that need to be discussed with counsel are listed in "What to Watch Out For" below).



WHAT TO WATCH OUT FOR

- Distribution arrangements with competitors.
- Exclusive arrangements for the purchase or sale of products or services.
- Selective price discounting to only certain customers.
- Bundling of services.
- Agreements that restrict a customer's choices in using a Coface service.
- Agreements to add a Coface employee to another entity's board of directors.



IN PRACTICE

You are working in Coface's commercial team and you receive a call from an executive of a competitor company. They tell you that it would be convenient for both to stop "fighting" for the clients and to distribute them artificially. What do you do?

You are in a meeting of your local insurance association and during the discussion some members of other companies start disclosing their sales projections, pricing policies and other key information about their business. They ask you to do the same. What should you do?

During a conference, one of your competitors asks if they can talk with you about discounting a popular product or service. What do you do?

➤ Collusive behaviour is prohibited in almost every jurisdiction because it severely affects the competition on the market and the country's economy. If any collusion proposal is received, you should reject it immediately and report it to your local Compliance Officer.

➤ The exchange of sensitive information could lead to collusive conducts and therefore is strictly forbidden. In the example, you should explicitly reject the information request and ask for your opposition to be recorded in the minutes.

➤ Make it clear that you object to such a discussion. Excuse yourself from the conversation immediately and report the incident to your supervisor and Compliance Officer. You should avoid all discussions that relate to pricing or price-related issues, including discounts, with any competitor.



Compagnie Française d'Assurance pour le Commerce Extérieur
1 place Costes et Bellonte
92270 BOIS-COLOMBES FRANCE
www.coface.com