ETHICS & COMPLIANCE

CODE OF CONDUCT

EXTIME MEDIA





extime
MEDIA

EDITORIAL

ETHICAL REFLEX, THE RIGHT COURSE!

Ethics and compliance are defined as respect for Extime Media's values (responsibility, quality and integrity) and compliance with laws and regulations.

Before being a change in procedures, ethics and compliance are based on a cultural change. Each employee must adopt these values in their daily professional practice.

In all circumstances, the ethical reflex is the right course!



LOYALTY, A TWO-PARTY COMMITMENT

The signing of an employment contract (permanent or fixed-term contract, apprenticeship contract, etc.) entails compliance, by both the employee and the employer, with an obligation of loyalty involving the probity of both parties in the performance of the work.

This duty of loyalty applies to :

- throughout the duration of the employment contract, including periods of suspension (e.g. work stoppages, holidays),
- to all employees, regardless of their position,
- regardless of any clause appearing in the employment contract on this subject.

This obligation covers all kinds of behaviour on the part of both the employee (not harming or denigrating the employer, a Client , a supplier, a partner, etc., not disseminating confidential information, carrying on a competing activity without prior authorisation, etc.) and the employer (paying due wages and meeting deadlines, providing the employee with the agreed tasks, making available the appropriate equipment to carry out the expected work, etc.) that may cause unlawful harm to either party.

WHY AN ETHICS AND COMPLIANCE SYSTEM FOR EXTIME MEDIA?

OUR DEFINITION OF ETHICS AND COMPLIANCE

For Extime Media, ethics and compliance involve both
compliance with laws and regulations
but also respect for Extime Media's values:
Responsibility, Quality and Integrity.

For our company, ethics and compliance are a lever of trust with all our stakeholders.
and therefore a lever for performance!

Ethics and compliance are not adjustment variables: they are an Extime Media imperative that must be our daily hallmark in the way we conduct our business and wherever we operate.

That's why Extime Media deploys a global system in which information, awareness-raising and training are key levers to support you in deploying the approach daily.

A solid ethics and compliance program helps to preserve a positive corporate image, while limiting the risks to which the company may be exposed. It is therefore a factor of confidence for our employees, Clients and suppliers, and a guarantee of good governance for our shareholders.

The principles set out in this Code are intended to help all employees in their day-to-day professional practice.

These rules of ethics and compliance are based on three principles that must guide our working behaviour: responsibility, integrity and respect for others.

Any breach of these rules may result in disciplinary action.

When faced with a delicate situation, it is therefore essential to discuss it with your managers or with the Ethics and Compliance Referent (see the chapter on "How to deal with a delicate situation"). Questioning one's own practices and discussing these issues are the keys to acquiring the right reflexes, finding the right solutions, detecting risky situations and reporting them to help the company move forward together!

It's the actions of each and every one of us that will keep us on course!



Ethics and compliance are now a prerequisite for doing business.

Failure to comply can lead to exclusion from certain markets or a ban on borrowing from banks to finance our expansion.

All our stakeholders are attentive to our approach to ethics and compliance. The values of responsibility, quality and integrity are factors in the company's success.

Everyone is a player and ambassador for ethics and compliance at their level and in their missions. This responsibility on the part of each employee is the strength of the company: it is a strong marker which fuels its performance. The rules of this Code must therefore be applied by every employee and by anyone acting for or on behalf of the company (subcontractors, etc.). Employees must also ensure that the people under their responsibility comply with its principles.

The purpose of the ethics and compliance approach is therefore to protect all Extime Media employees.

As part of a control, whatever its nature (internal control, audit, internal investigation, control of authorities, etc.), every employee involved must cooperate actively.



EXAMPLES OF SANCTIONS IMPOSED FOR ACTS OF CORRUPTION

- CONVICTION OF AIRBUS : 2.9 billion $ in 2020

WHY THIS CODE AND HOW TO USE IT?

Extime Media operates in a demanding environment where seemingly harmless misbehaviour can have seriously damaging consequences (criminal, financial, commercial, reputational, etc.).

Furthermore, Extime Media wished to establish rules of conduct which, although not exhaustive, should protect both its employees and itself.

This Code applies to all Extime Media employees.

It provides concrete illustrations so that you can make them your own and apply them to your day-to-day professional practices.

WHO DEFINES AND MANAGES THE ETHICS AND COMPLIANCE PROGRAMME?

The Compliance and Legal Departments of Extime Media's shareholders co-pilot its deployment, with the support of the Ethics and Compliance Referent within the company.

WHO SHOULD YOU CONTACT IF YOU HAVE ANY QUESTIONS OR ARE IN A DELICATE SITUATION?

It is essential not to be left alone when faced with questions or a delicate situation!

Through dialogue, situations can be clarified, risks detected, and solutions found (see Chapter "How to deal with a delicate situation").

An alert system* is also available to you: it is mentioned in this Code and in the Charter for handling alerts, which can be accessed on the alert platform.

* https://alert.groupeadp.fr

Extime Media's shareholders made a commitment by signing the 10 principles of the Global Compact in 2003, on which they base the deployment of its policies.

THE 10 PRINCIPLES OF THE GLOBAL COMPACT

Human rights

1. Promote and respect the protection of international human rights law.
2. Ensure that we are not complicit in human rights abuses.

International labour standards

3. Respect freedom of association and recognise the right to collective bargaining.
4. Contribute to the elimination of all discrimination in respect of employment.
5. Contribute to the effective abolition of child labour.
6. To contribute to the elimination of all forms of forced or compulsory labour.

Environment

7. To apply the precautionary approach to environmental issues.
8. Take initiatives to promote greater environmental responsibility.
9. Encourage the development and diffusion of environmentally friendly technologies.

Combating corruption

10. Act against corruption in all its forms, including extortion and bribery.

extime MEDIA

CONTENTS

COMPLYING WITH LAWS AND REGULATIONS 8
COMBATING BREACHES OF PROBITY 11
PREVENTING CORRUPTION 13
PREVENTING INFLUENCE PEDDLING 17
BE VIGILANT ABOUT GIFTS, INVITATIONS AND BENEFITS 19
DETECT AND DEAL WITH CONFLICTS OF INTEREST 21
COMPLIANCE WITH THE CODE BY PARTNERS 23
PROTECTING INFORMATION AND PERSONAL DATA 24
RESPECT FREE COMPETITION AND COMBAT COLLUSIVE AND COERCIVE PRACTICES 30
RESPECTING OUR EMPLOYEES AND PARTNERS 35
HOW TO DEAL WITH A DELICATE SITUATION the company's whistleblowing system and the protection of whistleblowers 37
GLOSSARY 42

COMPLYING WITH LAWS AND REGULATIONS

There can be no ethics without compliance with laws and regulations.

All employees must, at all times, strictly comply with the applicable laws and regulations, as well as the contractual obligations imposed on them in the performance of their duties.



THE +

Regulatory compliance enables effective risk management and protects employees against any form of breach of probity.
It is imperative if we are to preserve the trust of our stakeholders in our business relationships, which are founded on transparency.

Focus: international sanctions

International sanctions (or embargoes) may be imposed on certain countries, individuals or sectors. All company employees are therefore required to comply with them. Failure to comply with international sanctions regulations can result in significant civil and criminal penalties for the employee, the company and its shareholders. It is therefore essential to contact the relevant Compliance and Legal Department and the Ethics and Compliance Referent if you have any doubts or questions.

For example,

I've been promoted to a new job, and as part of this, I'm being asked to help implement the advertising contract with an airport authority. My team tells me that we are subject to specific constraints that I am not familiar with.

What should I do?

You should discuss the matter with your manager and request any relevant information from the relevant Legal and Compliance Department and/or the company's Ethics and Compliance Referent .

GOOD PRACTICE

- Discuss with your manager the legal knowledge required for your position.
- If necessary for the performance of your duties, acquire a minimum knowledge of laws and regulations.
- Contact the relevant Legal and Compliance Department to identify the applicable regulations.
- Respect the delegations in force.

AREAS TO WATCH OUT FOR

If in doubt about the legality of a document or the application of a procedure :

- Seek advice from your manager or other employees in your department.
- Consult the relevant Legal and Compliance Department, the Ethics and Compliance Referent or your HR manager, as appropriate.

For example,

What should I do?

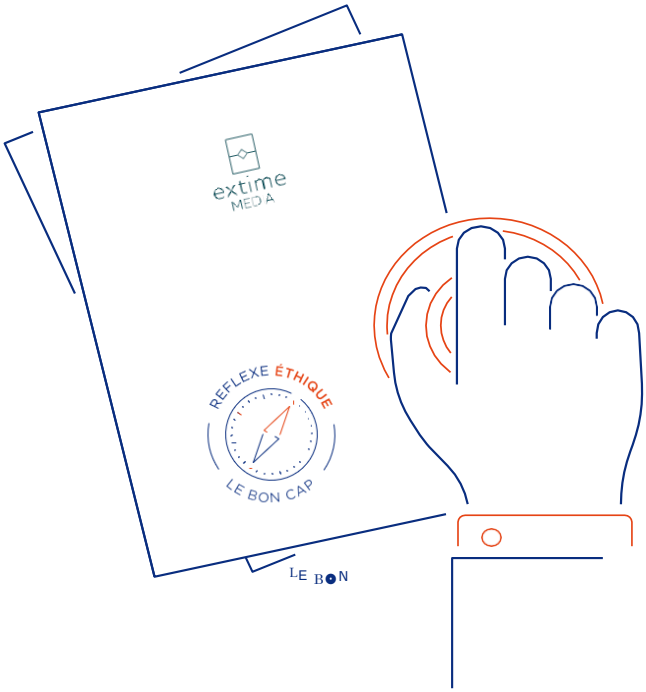
WHAT IS PROHIBITED

- Take a decision involving a legal risk without consulting your manager or the relevant Legal and Compliance Department.
- Commit yourself or the company if you have any doubts about compliance with laws and regulations.

COMBATING BREACHES OF PROBITY

Breaches of probity refer to any act of deception with the aim of obtaining an undue or illegal advantage.

They may be subject to criminal prosecution. They include theft, extortion, fraud, breach of trust, handling stolen goods, money laundering, corruption (see Chapter "Preventing corruption") or influence peddling (see Chapter "Preventing influence peddling")., favouritism, illegal interest-taking, misappropriation of public property or funds, insider dealing or misuse of corporate assets, concussion, collusion, coercive practices (see Chapter "Respect free competition and combat collusive and coercive practices"), obstructive manoeuvres, usurpation of identity and position.



For example,

I'm a management controller and, at 4pm on a Friday, I receive a call from someone claiming to be the Chairman and CEO, ordering me to make an immediate transfer to an account, the details of which he gives me.

Should I do it?

This could be a scam, known as "president fraud". You should follow procedures, inform your manager and launch any necessary checks.

For example,

I'm on a business trip and want to bring back a Gift for my children. I pay with my Corporate Business card and submit an expense report.

Is this acceptable?

This is a breach of trust to the detriment of the company.
The Corporate Business Card must be used for purely professional purposes, and no personal expenses may be charged.

GOOD PRACTICE

All employees must play their part in preventing fraudulent behaviour:

- Apply the instructions and procedures in force.
- Preserve the company's assets and inventory (equipment, materials, etc.).
- Keep track of your actions and keep supporting documents.

AREAS TO WATCH OUT FOR

- If you suspect fraud, inform your manager, the relevant Legal and Compliance Department or the company's Ethics and Compliance Referent .

WHAT IS PROHIBITED

- Agreeing to ignore company procedures.

PREVENTING CORRUPTION

Bribery consists of providing an advantage (gift, invitation, money, information, service, etc.) to a public or private person in order to obtain an act or abstention from that person. It can be active (on the side of the briber) or passive (on the side of the bribed). Intention alone is a corruption offence! Bribery involves the responsibility of the employees involved (briber and bribe-taker) as well as that of the company and its representatives. It also damages their reputation. To prevent corruption, three principles must be upheld and applied by all employees:

Zero tolerance, all concerned, all vigilant.

Extime Media will always be on the side of employees of integrity who refuse all forms of corruption.

GOOD PRACTICE

- Conduct day-to-day operations with openness, fairness and honesty, in accordance with Extime Media's operating standards.
- Share our commitment with our business partners.
- In the event of suspected or attempted corruption, inform your manager or the company's Ethics and Compliance Referent (see Chapter "How to deal with a delicate situation").

AREAS TO WATCH OUT FOR

- Feeling indebted following an advantage provided by a partner.
- Use intermediaries (or business introducers).
- Accepting or offering a gift or invitation without analysing the context (see Chapter "Be vigilant about gifts, invitations and benefits").

WHAT IS PROHIBITED

- Offering or accepting a "bribe", gift, invitation, service, etc. in order to obtain an order or in exchange for sensitive company information.
- Agreeing to retain an intermediary appointed by a client in order to win an order or a contract.
- Validating the receipt of a service or order in excess of that performed/supplied, with a view to obtaining an advantage from the supplier for oneself and/or for others.
- Considering entering into a business relationship without obtaining information about the third party in question (suppliers, customers, etc.)[1] .
- Making facilitation payments to speed up or facilitate the obtaining of an a authorisation (see Focus on "Bribery of public officials").

ONE EXCEPTION TO THESE PRINCIPLES: a tolerance is allowed when the physical integrity of the person or his/her close relations is threatened. In this case, inform your manager, your HR manager, the relevant Legal and Compliance Department or the Ethics and Compliance Referent as soon as possible.

[1] Procedure for assessing third parties

For example,

I work in the Technical Department and a supplier offers me VIP tickets for an event in exchange for information about our purchasing processes.

Is this acceptable?

For example,

I work in Sales and a Client says he's prepared to confirm an order for a campaign on condition that I agree to hire his son.

Is this acceptable?

FOCUS ON BRIBERY OF PUBLIC OFFICIALS

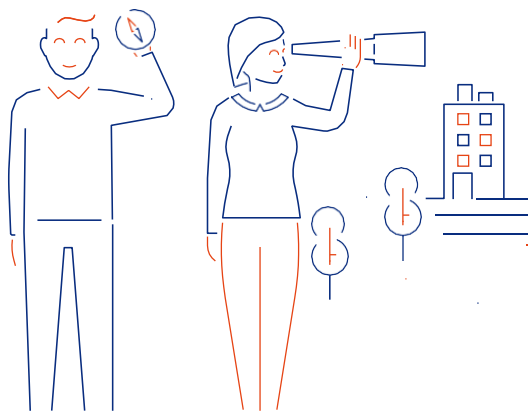
SANCTIONS IN FRANCE

FOR THE COMPANY

- Up to 5 million€ to 30% of turnover
- Market exclusions (by the World Bank, for example)
- Bans on borrowing
- Loss of reputation

FOR EMPLOYEES

- Up to 10 years of imprisonment
- Up to 1 million fine €
- Deprivation of civil rights
- Prohibition from carrying on the activity in question for 5 years or more



A public official is a person vested with public authority, entrusted with a public service mission or invested with an elective or jurisdictional mandate.
Beware, however, that this notion can be understood more

broadly depending on the country: it can concern the head of a public company, the head of a State monopoly or the senior executives of any company in which the State plays a dominant role.
Unwavering vigilance is therefore required, especially as bribery of public officials is more severely punished and may also fall under extraterritorial laws (which apply outside their country of origin) such as the US Foreign Corrupt Practices Act.



GOOD PRACTICE

- Carry out sufficient due diligence on third-party public officials who are particularly exposed to the risk of corruption.
- Conduct relations with public contacts in compliance with Extime Media's internal ethics and compliance system and local laws.
- In the event of suspected or attempted corruption, inform your manager or the company's Ethics and Compliance Referent .



WARNING AREAS

- Underestimating the risk of corruption by a public official because he is not a decision-maker, even though he may have access to sensitive information and/or influence the final decision.
- Paying too little attention to lobbying activities carried out by the company itself or by professional organisations
- Recruiting a former public official or someone close to them without considering the possible risk of corruption or influence peddling.
- Agreeing to work with a third party proposed by a public official in order to win a contract.
- Considering entering into a business relationship with a third party without carrying out the usual checks, on the grounds that the third party is recommended by a public official.

FACILITATION PAYMENTS

There is nothing trivial about making a payment to a public official or offering him a gift to guarantee or speed up the performance of a public act that he will have to carry out anyway. Considered a bribe in many countries, facilitation payments are prohibited in the corporate world.

It puts the company's reputation at stake and exposes it to legal risks and criminal prosecution under local and extraterritorial laws.



WHAT IS PROHIBITED

- Offering a public official a bribe, a gift, an invitation, a service, etc. in order to win a tender, speed up a decision, obtain information, etc.

For example

I work in the Technical Department and have to supervise the import of advertising devices to equip a platform. In order to speed up the customs procedure, a customs officer asks for a bribe.

What should I do?

This is incitement to corruption through the payment of a so-called "facilitation payment", which is strictly prohibited (see page 14). You must immediately inform your manager, the relevant Legal and Compliance Department and/or your Ethics and Compliance Referent.

PENALTIES FOR BRIBERY OF A PUBLIC OFFICIAL

IN TURKEY

- Revocation of business licence
- Ban on participating in invitations to tender and termination of the public procurement agreement
- Administrative fines
- Imprisonment of 4 to 12 years for employees involved

IN JORDAN

- Minimum 2 years of imprisonment for employees involved

IN THE USA

- Combination of criminal and civil penalties
- Up to $30 million per offence for companies
- Up to 25 years of imprisonment and a minimum fine of $6 million for employees

PREVENTING INFLUENCE PEDDLING

Influence peddling consists of soliciting a public person or a private person entrusted with a public service mission by providing them with an advantage so that they use their real or supposed influence with another person in order to obtain a favorable decision.

Intent alone can be classified as an offence. Like bribery, it can be active (on the part of the person soliciting) or passive (on the part of the person using their influence). The penalties are the same as for corruption.



GOOD PRACTICE

- Avoid any behaviour that could be perceived as a form of influence peddling, in particular by complying with the rules on gifts and invitations.
- Share our commitment with our partners in the context of our activities.



AREAS TO WATCH OUT FOR

- Allowing certain ambiguities to creep into relations with business partners.



WHAT IS PROHIBITED

- Offer an advantage of any kind (money, gift, invitation, service, etc.) to an elected official, a member of an administration, etc. so that they influence an acquaintance with a view to a decision, a vote, etc. in favour of Extime Media.
- Undertake, on behalf of the company, to finance political parties.
- Use intermediaries (business introducers) without informing the relevant Legal and Compliance Department and/or the company's Ethics and Compliance Officer.

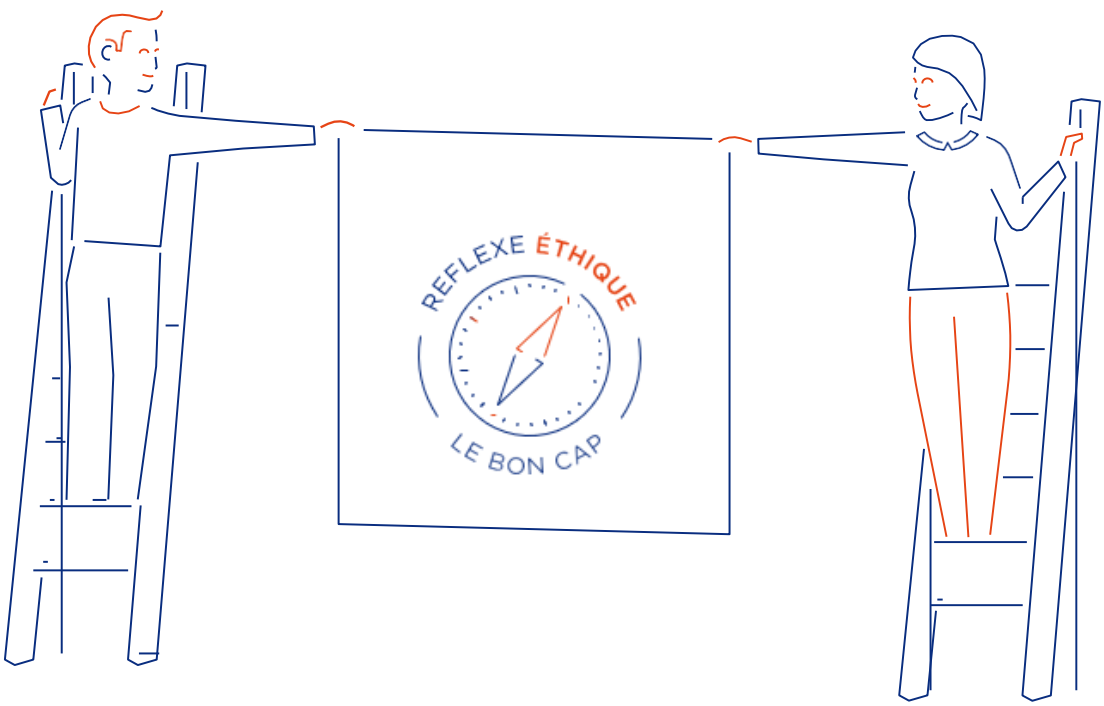
For example,

I work in the Technical Department and I am having difficulty obtaining an intervention permit from the prefecture for an operation.

As I personally know a member of the Minister's office, I am considering offering them an invitation to an event so that they can help me resolve the situation.

Is this acceptable?

This is an act of influence peddling prohibited by law and by the company's internal regulations.



BE VIGILANT ABOUT GIFTS, INVITATIONS AND BENEFITS

Gifts and invitations may be regarded as corruption. They must therefore remain exceptional.

While maintaining good relations may sometimes lead Extime Media employees to offer or accept gifts or invitations, it is essential to be able to decipher the context.

GOOD PRACTICE

- Analyse the context in which these gifts or invitations are offered/accepted according to the 4 criteria opposite.
- Give preference to promotional gifts or gifts of symbolic value.
- As far as professional seminars are concerned, if they are useful and beneficial to our business, Extime Media can finance the corresponding transport and accommodation.
- Systematically declare gifts and invitations offered to clients and, for those of a value of> 130€ , systematically request prior authorisation from your manager.
- Systematically declare gifts and invitations offered to suppliers and partners and, for those with a value > €70, systematically request prior authorisation from your manager.
- Systematically declare to your manager any gifts and invitations received worth > €70.
- Systematically ask your manager for authorisation for any exceptions to the above amounts.

WATCH OUT FOR

- Avoid any gift or invitation that would lead an outside observer to doubt the integrity of the giver or recipient.
- Avoid gifts or invitations likely to affect the impartiality of decisions that the employee must take in the interests of the company.

WHAT IS PROHIBITED

- Accepting a sum of money, even in the form of a loan or deposit, or the provision of movable or immovable property, equipment, travel or any other service free of charge from a third party, for yourself, a member of your family or your personal or professional circle.
- Accepting an invitation or gift that would place you in a position of obligation.
- Accepting a gift or invitation during a sensitive period (call for tenders or consultation, election period, negotiations with suppliers, etc.).

REFERENCES

The 4 criteria for analysing the context :

1 Contact the relevant Legal and Compliance Department and/or the Ethics and Compliance Referent to find out whether local law sets a specific framework.

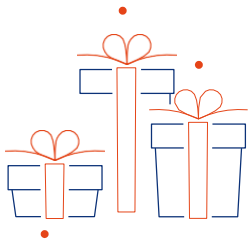
2 Identify the strategic context: do not accept or offer any gifts or invitations during periods of invitations to tender or consultation, elections, negotiations with suppliers, etc.

3 Stay within a professional framework and do not go beyond the private sphere. For example, the following is no longer business-related:

- An invitation that includes close relations or people who are not directly involved in the matter.
- In a seminar, when leisure time is greater than the time devoted to professional exchanges.

4 Define whether the amount of the gift or invitation is reasonable.

- Reciprocity test: am I capable of returning the same level of gift or invitation in the context of my duties?
- Reasonableness can also be assessed by taking into account local laws, the local standard of living, etc. This benchmark is particularly important abroad. For example, 5% to 10% of the average salary in other countries.



DETECTING AND DEALING WITH CONFLICTS OF INTEREST

A conflict of interest is a situation where the personal interests of an employee or someone close to him or her compete with the duties or tasks entrusted to him or her by the company. The employee can therefore no longer be impartial in his or her professional decisions. While conflicts of interest do not constitute an offence as such in most countries, they often give rise to delicate situations that can result in criminal offences.

Conflicts of interest can arise at any time in a person's life: a relationship with an external partner, a relationship within a team, the recruitment of a close relative, etc.



GOOD PRACTICE

- Carry out your duties in the strict and sole interest of the company, and never on the basis of personal interests.
- Know how to detect an emerging conflict of interest.
- Declare any conflict of interest, even a presumed one, to your manager or the Ethics and Compliance Referent and, with their help, determine how best to deal with the situation in order to reduce the risk for the employee and the company.



AREAS TO WATCH OUT FOR

- Be attentive to your close entourage and employees who may have business or personal relations or financial interests with a supplier, competitor or customer of Extime Media.
- In the context of certain public commitments (elected office, associations, etc.), be careful not to take part in decisions concerning Extime Media.



WHAT IS PROHIBITED

- Concealing a conflict of interest that would expose the company or the employee.

For example

I am involved in the selection of a supplier. One of the candidate companies employs my brother.

What should I do?

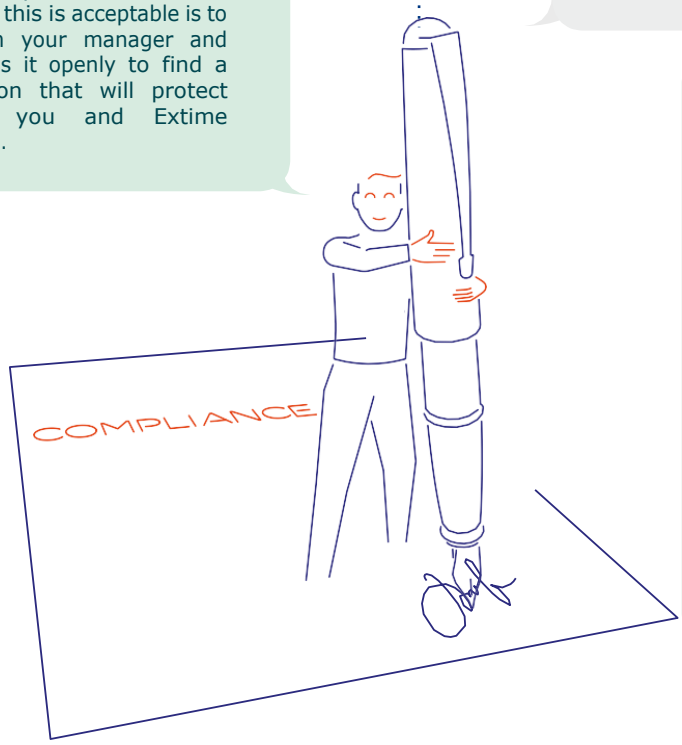
Given your brother's position in this company and the financial stakes involved, there could be a conflict of interest if your brother is a salesman in this company, for example. The only way to know whether or not this is acceptable is to inform your manager and discuss it openly to find a solution that will protect both you and Extime Media.

For example,

In my spare time, I'm President of an association campaigning for the protection of the environment and against the development of aviation.
At Extime Media, I'm in charge of a corporate communications project for a new airport hub .

How should I behave?

Extime Media respects the privacy of its employees and encourages them to get involved in community life.
However, you must inform your manager of your membership or involvement in such an organisation if you believe that there is, or could be, a conflict with the company's interests. Your manager or your Ethics and Compliance Referent will be able to advise you on the appropriate course of action.



COMPLIANCE WITH THE CODE BY PARTNERS

Extime Media attaches great importance to the relationships it maintains with its many partners. These relationships must be based on respect for contractual obligations and rules of good conduct.

The company's partners are therefore invited to implement a set of appropriate policies aimed at preventing breaches of integrity (see Chapter "Combating breaches of integrity").

In this context, the commercial partner may be asked for information concerning the subjects covered by this Code and it may be decided to implement remedial measures in the event of a breach (audit, review/termination of the contract, etc.).

Any breach of this Code must be reported via the alert system accessible to our employees and service providers at https://alert.groupeadp.fr.



GOOD PRACTICE :

- Ensure that the assessment of the third party has been carried out before the contract is signed, in accordance with the procedure and operating method in force.
- Ensure that the remedial actions decided by the company are properly applied (questionnaire, sharing of internal Ethics and Compliance policies, contractual clauses, etc.).
- Contacting the relevant Legal and Compliance Department prior to any contractual arrangements, in particular to negotiate the Ethics and Compliance clauses.
- Send the dedicated Code of Conduct to suppliers at the start of negotiations.



AREAS TO WATCH OUT FOR :

- In the event of a suspected deviation from this Code or the Supplier Code of Conduct or the contract, notify the manager or the company's Ethics and Compliance Referent in order to deal with the situation (additional information or questionnaire, audit, contract review, etc.).



WHAT IS PROHIBITED?

- Signing a contract without having assessed the third party in accordance with the Third Party Assessment procedure, or consulted the relevant Legal and Compliance Department and/or the Ethics and Compliance Referent beforehand.
- Ignore the recommendations of the Ethics and Compliance Referent .

PROTECTING INFORMATION AND PERSONAL DATA

The various activities carried out within Extime Media are based on the daily exchange and processing of data, facts, statistics and studies relating to the company's business. This wealth of information is an asset. Leaking information, or processing it incorrectly or without proper control, can have damaging consequences for the company.

Protecting these assets is essential if our company is to develop and remain competitive. It is essential to control and protect sensitive company information, whatever its nature, medium or location.

The company has drawn up a "Charter for the use of IT resources and social media". Its day-to-day implementation is everyone's responsibility. Each employee's involvement must contribute to ensuring that it is respected.



THE +

Information security makes it possible to preserve the digital ecosystem in order to protect the company and all its stakeholders, as well as its image and reputation.

In this context, the protection of personal data reflects our commitment to offering our stakeholders secure services that respect their rights to their data (confidentiality, privacy).

The transparency, quality, integrity and security of personal data are factors of confidence in the responsible processing of personal data.

THE SPECIFIC CASE OF PERSONAL DATA

Any data or information relating to an identified or identifiable natural person constitutes "personal data". An individual may be identified directly (e.g. surname, first name) or indirectly (e.g. email address, telephone number, vehicle registration number, badge number), by a single piece of data (e.g. name) or by combining several pieces of data (e.g. a woman living at such and such an address, born on such and such a day and a member of such and such an association). Some personal data is sensitive (national insurance number, biometric data, health data, etc.).

Any operation carried out on personal data constitutes "processing of personal data" (collection, access, consultation, use, modification, deletion, storage, etc.).

All processing of personal data by Extime Media employees must comply with the main principles of the General Data Protection Regulation (GDPR) to which the company is subject (see table below), as well as the practices in place within the company. The Data Protection Officer (DPO) is your key contact, with the support of the relevant Legal and Compliance Department, to help you ensure compliance with the regulations.

THE MAIN PRINCIPLES OF PERSONAL DATA PROTECTION

1. Lawfulness and purpose: personal data must be processed lawfully (for valid reasons) and for specified purposes, and may not be further processed in a way incompatible with those purposes.

2. **Minimisation**: only personal data that is adequate, relevant and strictly necessary for the defined purpose may be processed.

3. **Limits on storage**: the storage period must be set according to the type of personal data processed and the purpose defined. The data must then be deleted or made anonymous.

4. **Security**: appropriate security measures must be put in place to guarantee the integrity, availability and confidentiality of the personal data processed. In particular, only authorised persons may have access to personal data.

5. **Respect for the rights of individuals**: individuals whose personal data is processed by the company must be informed in a transparent manner of the terms and conditions of such processing and of their rights.

PENALTIES FOR BREACHES OF PERSONAL DATA PROTECTION

Administrative fines :

- Maximum €10 million or 2% of the previous year's consolidated turnover for common infringements (breaches of the obligations of the controller and processor).
- Maximum €20 million or 4% of the previous year's consolidated turnover for failure to comply with fundamental principles, the rights of individuals, and obligations when transferring data to third countries or international organisations.

Civil penalties (compensating the persons concerned in the event of damage suffered) or criminal penalties (particularly in the event of failure to comply with safety obligations) may also be imposed.

PROTECTING INFORMATION AND PERSONAL DATA (CONTINUED)

GOOD PRACTICE

- Observe the principle of discretion with regard to company information, both inside and outside the company.
- Assess and indicate the level of confidentiality of the information contained in the documents produced.
- Ensure that it has a secure IT connection in accordance with the company's or shareholders' requirements.
- Maintain traceability of exchanges of the most sensitive documents.
- Store and destroy your documents using resources appropriate to their level of confidentiality (strongbox, shredder, etc.).

And for personal data:

- Identify the personal data you use or to which you have access in the course of your work, right from the start of a project.
- Protect the confidentiality of data and do not pass it on to anyone, including internal staff, without checking that they are authorised to receive it.
- Not to transfer personal data stored on company systems to personal equipment or storage spaces.
- Comply with all confidentiality and security instructions and rules communicated to you by the company.
- Contact the DPO if you are in charge of a file involving new processing of personal data (or the modification of existing processing), or as soon as you have any doubts about the use, access or transmission of personal data.

AREAS TO WATCH OUT FOR

- When you telework or are on an assignment, follow the instructions laid down by the company.

What about personal data?

- In the event of theft, loss of data (e.g. stored on a USB stick) or alteration of data (e.g. following unlawful access), immediately inform your dedicated Security and Data Protection contacts (RSSI and DPO).

WHAT IS PROHIBITED

- Communicating in any form whatsoever, without a legitimate reason and without appropriate protection measures, any sensitive information concerning the activity of Extime Media and its subsidiaries without the prior authorisation of the manager.
- Giving precise information about the projects you are working on or have worked on on social networks.

And for personal data:

- Reuse personal data for purposes other than those initially intended, in particular for commercial purposes.
- Communicating this data to persons, both internal and external, who are not among the identified and authorised recipients.
- Keep personal data beyond the period defined in the register, in particular on a hard disk or other mobile medium.

Information on data protection

1 PASSWORDS

Create complex passwords, different for each use, and never share them with anyone.

2 BACKUP

Save your business data only on the company's storage spaces

3 UPDATING

Apply the IT department's instructions for updating your hardware as soon as possible.

4 Removable media

Avoid using removable media and do not store confidential data on them (risk of loss and spread of malware); prefer to use a secure file exchange platform.

5 MESSAGING

Report any suspicious messages to your IT department: look out for links and attachments before clicking.

6 DOWNLOADS

If in doubt, don't click on the link and have your IT department check it out

7 NOMADISM

Data is not stored on your PC, but on storage spaces provided by the company; use a confidentiality filter on your screen.

8 SEPARATION OF USES

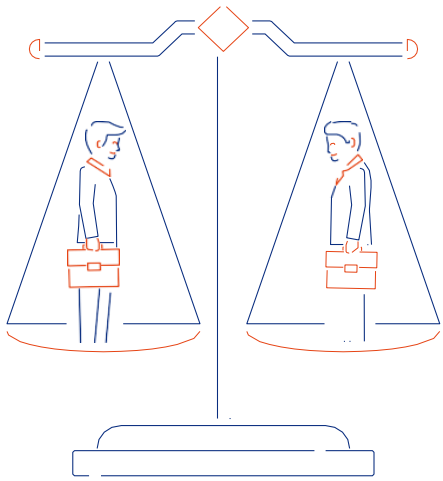
Separate your professional and personal uses: email, equipment, storage, etc.

9 MALWARE

Switch off your computer in the event of unusual behaviour and contact IT support.

RESPECT FREE COMPETITION AND COMBAT COLLUSIVE AND COERCIVE PRACTICES

Open and undistorted competition is the guarantee of healthy and fair commercial relations.
Competition law, particularly in Europe, prohibits price fixing, market sharing, the exchange of strategic information between competitors, and the abuse of a dominant position.
It requires equal treatment of economic players operating in the same market.
The company's relations with its many commercial partners are based on the principles of fairness, transparency and non-discrimination.
Failure to comply with these rules can result in severe penalties for both the employee and the company.



For example,

During a conference, a colleague from another airport told me that he would like to be able to share airport best practices with me. As this seemed useful to me, we decided to exchange information by e-mail every month.

Is this acceptable?

Exchanges of commercially sensitive information, i.e. non-public, current or future, individual and non-aggregated information relating to business confidentiality, are prohibited and may be punished. This information relates in particular to pricing strategy, costs and commercial policy vis-à-vis airlines.

Consulting the relevant Legal and Compliance Department will help you decide what is and isn't possible.

COMPETITION LAW SANCTIONS

France and Europe :

For employees who are personally liable

- For the most serious cases, up to 4 years of imprisonment
- € 75,000 fine

For the company

- Up to 10% of its consolidated worldwide turnover
- Nullity of the agreement or disputed clauses
- Action for damages
- Exclusion from tendering procedures
- Loss of reputation

THE +

Fair and equitable competition in our business relationships guarantees the confidence of all our stakeholders.
It is essential to the company's success, and guarantees its reputation.

COLLUSION

Collusion refers to practices (agreements, associations, etc.) between economic players aimed at distorting or even preventing free competition in a public procurement procedure. The aim of all these practices is to enable a predetermined candidate to win a contract.

GOOD PRACTICE

- Act fairly with our partners (suppliers, clients, businesses, etc.) by providing everyone with the same information.
- If in doubt about the practices of a partner or competitor, consult their manager, the relevant Legal and Compliance Department or the Ethics and Compliance Referent in order to assess the risks that may exist and determine the appropriate course of action.

AREAS OF VIGILANCE

- Report any suspicion of unfair competition or collusive practices to your manager.
- Give rebates, discounts and financial advantages in any form whatsoever without following the appropriate procedures.

WHAT IS PROHIBITED

- Exchanging, directly or indirectly, strategic information with competing economic operators.
- Facilitating, directly or indirectly, the communication of commercially sensitive information between competing customers, economic operators or suppliers.
- Participating in meetings with the customer during the tender period outside of any hearing procedure organised and validated for all candidates, unless the meeting concerns a contract in progress.
- Providing service offers of convenience in order to win a contract.
- Organising regular informal meetings with authority officials during a call for tenders.
- Agreeing between candidates on the content of bids in advance (particularly on price, geographical distribution of contracts, etc.).

PENALTIES

EXCLUSION

EUROPEAN UNION

Collusion between economic operators is prohibited by EU law. Candidates who engage in collusive practices may be excluded from tender procedures between EU Member States. Such practices may also lead to legal proceedings.

WORLD BANK GROUP

Exclusions prohibit the supplier from contracting with any World Bank Group (WBG) institution or any organisation whose activities are financed or advised by the WBG.

These exclusions may be accompanied by financial penalties.

For example,

Our consultant took part in informal discussions on the prices of bids with the local authority managing a call for tenders for the award of a contract at the airport. **Can our company be penalised as a result of these discussions?**

Yes, it can be considered that the final price of the company's bid depended on the discussions that the consultant had with this authority. This is a collusive practice contributing to unfair competition.

- **FOCUS ON COERCIVE PRACTICES**

A coercive practice consists of influencing the actions of a person or legal entity by harming them or their property, or threatening to do so.

Sanction: These practices may be sanctioned by European or international institutions.

For example,

In the context of a new contract, competing candidates tried to intimidate the Extime Media employee in charge of the file into withdrawing the bid, going so far as to threaten him.

Is this acceptable?

These are coercive manoeuvres and a serious breach of free competition. They must be reported in order to be punished.

- **FOCUS ON FAVOURITISM**

In France, there is a specific offence of favouritism in the context of public procurement. It consists of the simple act of "procuring or attempting to procure for another person an unjustified advantage by an act contrary to the legislative or regulatory provisions intended to guarantee freedom of access and equality of candidates in contracts and concessions".

Penalty: In France, this is punishable by two years of imprisonment and a fine of €200,000.

For example,

An employee sends supplier A a quote from another supplier B to see if he can match the price.

Is this acceptable?

No, this prevents competition and favours supplier A who, by offering a lower quote, is certain to get the order.

This is an offence of favouritism.



GOOD PRACTICE

- Put all purchases out to tender in accordance with the company's procedures.
- Call on the Purchasing Department or the Finance Department for all purchases, whatever the amount.
- Provide a precise and objective description of requirements when making a purchase.



AREAS TO WATCH OUT FOR

- In the event of relationships with suppliers that are not strictly professional, do not take part in the procedure (in particular, do not judge applications and tenders).
- Refrain from passing on to the outgoing incumbent any information about the consultation in progress other than that passed on to all the suppliers consulted.
- Demonstrate objectivity in describing requirements and analysing tenders (any judgement must be reflected in the tenders submitted).



WHAT IS PROHIBITED

- Accepting an invitation/gift offered by a consulted supplier.
- Rejecting the offer of a supplier consulted without giving any reasons even though it was the best bidder.
- Favouring a consulted supplier by providing it with information to help it prepare its offer.
- Modifying the rules of the procedure in order to favour a consulted supplier.
- Orienting its requirements so that only a consulted supplier is in a position to respond to the call for competition.

RESPECTING OUR EMPLOYEES AND PARTNERS

Respecting our employees contributes to their well-being and therefore to our success. With this in mind, it is particularly important to combat discrimination and harassment.

Treating our partners with the same respect fosters trusting collaboration.



GOOD PRACTICE

- Listening to our employees and colleagues and treating them fairly.
- To create conditions conducive to trust and dialogue in order to better manage delicate situations within our teams. For example, encouraging discussions rather than emails whenever possible, writing emails clearly and courteously, and limiting the sending of emails outside office hours, except in emergencies.
- Be respectful of others: treat our colleagues, partners and customers in accordance with the company's major commitments.
- Inform your manager, HR Manager or the Ethics and Compliance Officer in the event of harassment or discrimination.
- Share our ethical commitments in the broadest sense with our partners and do not hesitate to discuss these issues with them.



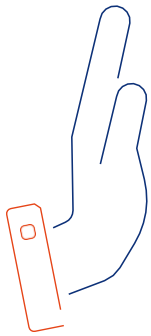
AREAS OF VIGILANCE

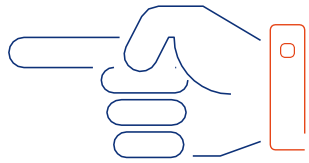
- Listening for weak signals to detect situations where our employees are unhappy.
- Detecting and reporting any deviations by our partners from our ethical principles.



WHAT IS PROHIBITED

- Discriminate directly or indirectly, particularly when hiring or promoting employees.
- Adopting any behaviour that could be perceived as harassment or sexist behaviour.





For example,

A member of staff hasn't selected a supplier that seems to me to meet all our expectations. Given the comments he often makes, I suspect it's because of the nationality of the company manager.

What should I do?

Any discrimination based on gender, skin colour, nationality, ethnic origin or sexual orientation is unacceptable. You should report it to your manager or your Ethics and Compliance Officer.

For example,

My line manager systematically criticises and belittles the quality of her female employees' work to the point where they have lost all confidence in themselves, even though they have always been recognised as highly competent.

What can I do about this?

Part of a manager's role is to stimulate and motivate his or her team, which includes treating everyone fairly and objectively. A manager has a duty to set an example by treating team members, individually and collectively, with respect and objectivity.

If you witness or are the victim of psychological and/or sexual harassment, don't keep it to yourself. Talk to your Harassment Officer, your HR Manager or your Ethics and Compliance Officer.

SANCTIONS IN FRANCE

DISCRIMINATION :

- Up to 3 years of imprisonment and a €45,000 fine

HARASSMENT :

- Up to 3 years of imprisonment and a €46,000 fine

HOW TO DEAL WITH A DELICATE SITUATION? the company's whistleblowing system and the protection of whistleblowers

A company's image is essential to the development of its activities and its performance. Every employee contributes to its reputation through his or her behaviour or statements.
Whistleblowing enables the company to take a forward-looking approach while protecting its interests and those of its employees. The purpose of whistleblowing is to enable employees or external partners and co-contractors (in particular suppliers, customers, service providers and subcontractors) to report serious and specific malfunctions, the scope and conditions of use of which are strictly governed by laws[2] , regulations and internal procedures such as the Whistleblowing Charter. Whistle-blowers benefit from legal protection guaranteed by the processes put in place (anonymity, protection against reprisals, penalties for those who violate the principles of whistle-blower protection, etc.).

Who can I contact? How can I contact them?

You can ask questions or report a breach of the principles of this code to :

1/ the Ethics and Compliance Officer of the company and its two shareholders via the alert system using the https://alert.groupeadp.fr platform, anonymously or not.

2/ your managers,

3/ the department responsible for the matter: Human Resources Department, Legal and Compliance Department, etc.

How does the company manage ethical alerts?

The company handles any alert it receives:

- With neutrality, impartiality, objectivity and proportionality.
- By formalising its process: cf. alert handling charter
- While respecting the confidentiality of the identity of the persons and information and the rules of data protection (of the whistleblower, any facilitator[3] , all individuals at risk of reprisals in the context of their professional activities). They are protected throughout the processing of the alert and after its closure. Any breach of confidentiality by those responsible for handling alerts is punishable by criminal penalties.

[2] Law no. 2016-1691 of 9 December 2016, known as the SAPIN II Law, Law no. 2017-399 of 27 March 2017 on the duty of care of parent companies and ordering companies, and Law no. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers.

[3] Any natural or legal person who has participated in facilitating the disclosure or reporting by a whistleblower.

GOOD PRACTICE

- Report breaches of the company's laws, regulations, codes and procedures.
- Make a precise, factual and detailed report, so that the Ethics and Compliance Referent can check whether the alert is admissible. Failure to do so may result in the alert being declared inadmissible.
- Reporting in good faith and without direct financial consideration. The use of this whistleblowing system in good faith, even if the facts subsequently prove to be inaccurate or do not give rise to any follow-up, does not expose the person making the report to sanctions.

AREAS TO WATCH OUT FOR

- Having doubts or questions.
- Not feeling concerned by a breach:
  - A report that is not dealt with internally may lead to a report being made to an authority and further expose the company.
  - A report may come from outside the company and therefore damage its image.

WHAT IS PROHIBITED

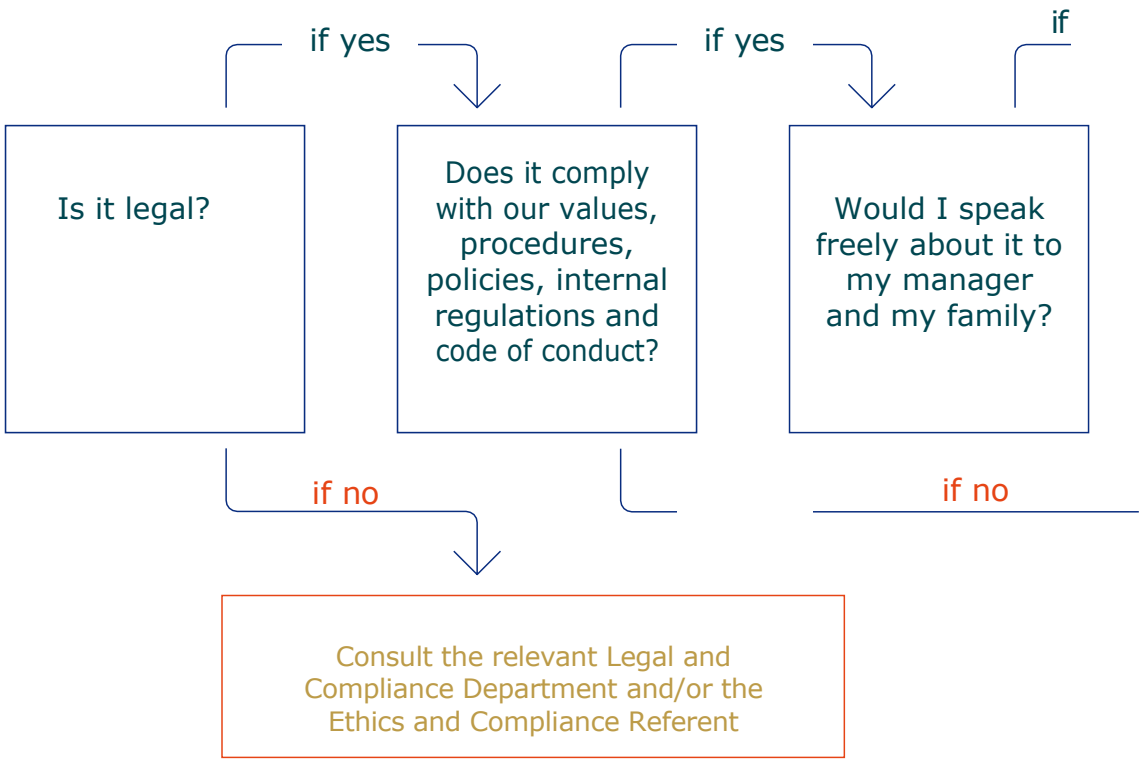
- Escalating or reporting mere suppositions, rumours or personal grievances. Any misuse of this whistleblowing system may expose its author to disciplinary and/or legal measures.
- Obstructing an alert or harming its author.

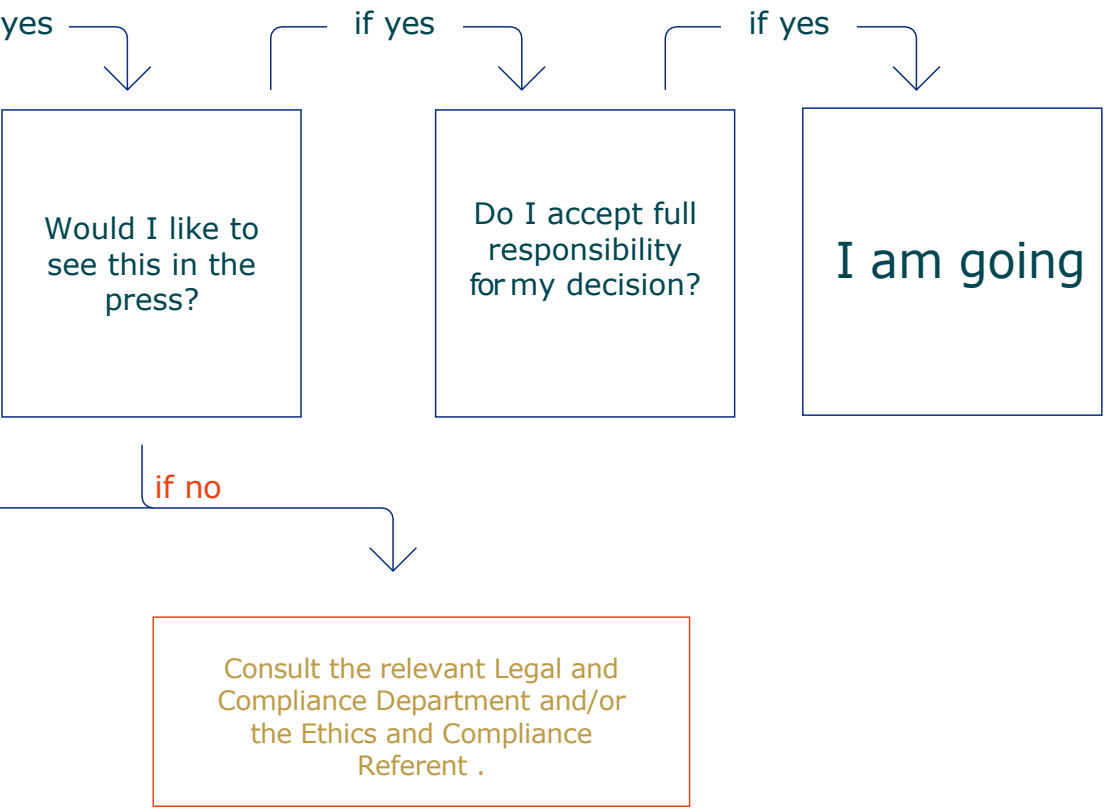
PENALTIES

- Reprisals against a person because of his or her status as a whistleblower :
  - Up to 3 years of imprisonment and a €45,000 fine
- Abusive or dilatory proceedings against a whistleblower because of the information reported or disclosed :
  - Civil fine of up to 20% of the claim for damages. If no claim is made, a fine of up to €60,000.
- Disclosure of confidential information relating to the identity of the persons making the report, the persons concerned by the report and the information gathered by all the recipients of the report:
  - Up to 2 years of imprisonment and a fine of €30,000.
- Obstructing, in any way whatsoever, the transmission of an alert :
  - Up to 1 year of imprisonment and a fine of €15,000

Never be left alone in a difficult situation

Questions to ask myself:




yes
Would I like to see this in the press?
if yes
Do I accept full responsibility for my decision?
if yes
I am going
if no
Consult the relevant Legal and Compliance Department and/or the Ethics and Compliance Referent .

USEFUL LINKS

Alert system
https://alert.groupeadp.fr

Intranet site
https://jcdecaux.sharepoint.com/sites/Extime-JCDecauxAirport

You will have access to :

- procedures enabling you to apply the various issues in your professional practice
- all the reference documents
- the latest news
- contacts

GLOSSARY

MISUSE OF CORPORATE ASSETS

Misuse of corporate assets is an offence committed by company directors who, in bad faith, use the company's assets or credit in a way that they know to be contrary to the company's interests, for personal gain or to favour another company or business in which they have a direct or indirect interest. This offence is punishable by 5 years' imprisonment and a fine of €375,000.

BREACH OF TRUST

Breach of trust is the act of disposing of property belonging to someone else in a way that is contrary to what was agreed with the owner. An example would be the use of property entrusted by the company (bank card, vehicle, etc.) for personal purposes without this being expressly provided for. This offence is punishable by 3 years' imprisonment and a fine of €375,000.

ADVANTAGE INDU

This is an advantage, in any form whatsoever (money, service, gift, invitation, etc.), for which there is no counterpart in the legitimate relationship; example: a payment of money that does not correspond to payment for a good or service.

MONEY LAUNDERING

Money laundering involves concealing funds of illicit origin (drug trafficking, theft, fraud, tax evasion, etc.) by reinvesting them in legal activities (real estate, catering, etc.). This offence is punishable by 5 years' imprisonment and a fine of 375,000€ , which can be increased in the most serious cases to 10 years' imprisonment and a fine of 750,000€ .

COLLUSION

This refers to illicit agreements between economic operators aimed at distorting or even preventing free competition in the procedure for awarding a public contract.

CONCUSSION

Concussion is an offence consisting of obtaining the delivery of funds or property of any kind, or a signature, an undertaking, a waiver or the revelation of a secret, by means of violence, threats or coercion. In the legal sense, it involves embezzlement in the exercise of a public function, particularly in the handling of public funds. This offence, committed by a natural person, is punishable by 5 years' imprisonment and a fine of €500,000, which may be increased to double the proceeds of the offence. For a legal entity, the fine is €2,500,000, which can also be doubled.

CORRUPTION

Bribery consists of providing an advantage (gift, invitation, money, information, etc.) to a public or private person in order to obtain an act or abstention from that person. It can be active (on the side of the briber) or passive (on the side of the bribed). This offence is punishable by 10 years' imprisonment and a fine of €1 million for individuals.

OFFENCE OF FAVOURITISM

Favouritism occurs when a person procures or attempts to procure for another person an unjustified advantage by an act contrary to the rules guaranteeing freedom of access and equality of candidates in public contracts and delegations of public services.

INSIDER TRADING

Insider dealing is an offence relating to the financial markets. It occurs when a person carries out a stock market transaction (purchase or sale) on the basis of information that has not yet been made public. Insider dealing is punishable by 5 years' imprisonment and a fine of up to €100 million.

MISAPPROPRIATION OF PUBLIC PROPERTY OR FUNDS

Misappropriation of public funds is the illegal use of sums or property belonging to the community for purposes other than the public good. The act by an official of destroying, embezzling or misappropriating public funds or property entrusted to him by virtue of his duties or mission. This offence, committed by a natural person, is punishable by 10 years' imprisonment and a fine of €1,000,000, which may be increased to twice the amount of the proceeds of the offence. If the offence is detrimental to the financial interests of the European Union, the fine is €2,000,000, which may be doubled. For a legal entity, the fine is €5,000,000, which may be doubled.

DUTY OF LOYALTY

The signing of an employment contract (permanent contract, fixed-term contract, apprenticeship contract, etc.) entails compliance by both the employee and the employer with a duty of loyalty involving the probity of both parties in the performance of the work.
The duty of loyalty requires the employee not to commit any act likely to be prejudicial to the company. The duty of loyalty is generally accompanied by an obligation of loyalty or confidentiality.

FRAUD

Fraud is the act of deceiving a natural or legal person, either by using a false name or capacity, or by abusing a true capacity, or by using fraudulent manoeuvres, in order to induce that person to hand over funds, securities or any other property whatsoever, to provide a service or to consent to an act. This offence is punishable by 5 years' imprisonment and a fine of 375,000€ .

EXTORTION

Extortion is the act of obtaining by violence, threat of violence or coercion either a signature, an undertaking or a waiver, or the revelation of a secret, or the handing over of funds, securities or any other property.

FACILITATOR

Any natural or legal person involved in facilitating the disclosure or reporting by a whistleblower.

WHISTLE-BLOWER

A whistleblower is a natural person who reports or discloses, without direct financial consideration and in good faith, information relating to a crime or misdemeanour, a threat or harm to the general interest, a violation or attempted concealment of a violation of an international commitment duly ratified or approved by France, a unilateral act of an international organisation taken on the basis of such a commitment, a violation of European Union law, a law or regulation.

Whistleblowers enjoy legal protection against reprisals (from their employer, for example) and criminal prosecution, provided they act in good faith.

OBSTRUCTIONIST TACTICS

Obstruction is defined as an act aimed at deliberately destroying, falsifying, altering or concealing any evidence in an investigation, or making false statements to investigators in order to obstruct an investigation.

FACILITATION PAYMENT

This involves paying a sum of money, usually to a public official, in order to facilitate an administrative procedure (e.g. obtaining a permit) without this being provided for in the normal procedures. In many countries, this type of behaviour is considered a corruption offence.

COERCIVE PRACTICES

This consists of harming or causing damage, or threatening to do so, directly or indirectly, to a party or to property of that party in order to unduly influence the actions of a party.

STAKEHOLDERS

A stakeholder is a group of individuals who can influence or be influenced by the achievement of a company's objectives. Stakeholders have a direct or indirect relationship with the company.
Stakeholders may be internal (managers, employees, directors, etc.) or external (shareholders, partners, customers, suppliers, competitors, etc.).

ILLEGAL ACQUISITION OF INTERESTS

Illegal acquisition of interests is the act, by a person holding public office or entrusted with a public service mission, or by a person holding a public elective office, of taking, receiving or retaining, directly or indirectly, any interest whatsoever in a company or in a transaction for which, at the time of the act, he or she is responsible, in whole or in part, for overseeing, administering, liquidating or paying. This is an offence committed by a natural person and punishable by 5 years' imprisonment and a fine of €500,000, which may be increased to double the proceeds of the offence. For a legal entity, the fine is €2,500,000, which can also be doubled.

RECEL

Concealment is the act of concealing, holding or passing on a thing, or acting as an intermediary to pass it on, in the knowledge that the thing has come from a crime or misdemeanour. Concealment is punishable by 5 years' imprisonment and a fine of €375,000.

REPRESENTATION OF INTERESTS (OR LOBBYING)

Lobbying is defined by Transparency International as "any communication, written or oral, between a representative or interest group and a public decision-maker with the aim of influencing a decision".

BIDDER

A tenderer is an economic operator who submits a bid as part of a procedure for awarding a public procurement contract.

INFLUENCE PEDDLING

Influence peddling consists of soliciting a public person or a private person entrusted with a public service mission (such as Aéroports de Paris SA) by providing them with an advantage so that they use their real or supposed influence with another person in order to obtain a favourable decision. This offence, committed by a natural person, is punishable by 10 years' imprisonment and a fine of €1,000,000, which may be increased to twice the amount of the proceeds of the offence. If the offence damages the financial interests of the European Union, the fine is €2,000,000, which may be doubled. In the case of a legal entity, the fine is €5,000,000, which may be doubled.

USURPATION OF IDENTITY OR POSITION

This involves using one or more data of any kind to impersonate a third party with a view to disturbing their peace of mind or that of others. Usurpation of function is the act by any person acting without title, of interfering in the exercise of a public function by performing one of the acts reserved for the holder of that function.



ETHICS & COMPLIANCE

EXTIME MEDIA CODE OF CONDUCT

extime
MEDIA