March 20, 2019

COMPLIANCE PROGRAMME

for

ATLANTIA's FOREIGN SUBSIDIARIES

CONTENTS

DEFINITIONS, ABBREVIATIONS AND ACRONYMS

Atlantia: Atlantia S.p.A.

Atlantia Group: Atlantia and its Subsidiaries.

Corporate recipients: Executives, top and middle managers, administrative staff, blue-collar workers of each Subsidiary

Code of Ethics: Code of Ethics of the Atlantia Group

Foreign subsidiary (FS): Subsidiary controlled, directly or indirectly, by Atlantia S.p.A. that does not have its administrative headquarter or main business in Italy

Anticorruption Officer: Anticorruption Officer appointed by each Subsidiary.

Anticorruption Policy: The Anticorruption Policy adopted by Atlantia and its Subsidiaries

Organisational, Management and Control models: The Organisational, Management and Control Model pursuant to Legislative Decree 231/2001, adopted by Atlantia in order to prevent commission of the offences covered by the Decree

Compliance Programme (CP): Compliance model regarding corporate responsibilities for Foreign Subsidiaries of Atlantia

Areas at Risk: Areas of activity considered to be potentially at risk of corporate liability

Chief Executive Officer: Chief Executive Officer of the Foreign Subsidiary, or the individual/body assigned similar functions in accordance with the rules, applicable laws and charter or to which operative authorities are assigned.

FS Compliance Officer (CO): Compliance Officer appointed by each Subsidiary with the task of monitoring the Compliance Programme

General Counsel: Atlantia's General Counsel

Group Compliance Officer: Compliance Officer appointed by Atlantia, as part of the Group Compliance and Security department

Internal Audit Department: The Atlantia Group's Internal Audit department

Third Parties: Any party engaging in commercial and/or financial relations with the Company

1. Introduction

Atlantia S.p.A. ("Atlantia") is the holding company of a multinational group operating in the motorway and airport infrastructure sector and in different economic, political, social and cultural environments.

The Atlantia Group operates transport and communications infrastructure and networks throughout Italy and around the world.

In recent years, many countries have established a criminal or quasi-criminal corporate liability regime. Most of these regulations encourage companies to adopt corporate governance structures and risk prevention systems, also providing for an exemption or mitigation of applicable penalties in the event of the adoption of adequate preventive measures.

The Atlantia Group, fully aware of the negative effects of illegal practices within the economic and social development of the areas in which it operates, is committed to preventing and combating illegal activities in its business.

As part of its commitment in this area, the Atlantia Group has adopted the Code of Ethics and the Anticorruption Policy, which – in conjunction with the Organisational, Management and Control models adopted pursuant to Italian Legislative Decree 231/01 - sets out the values that inspire the Group in the pursuit of its objectives and the key principles underlying its management practices.

As further confirmation of its commitment in preventing criminal corporate liability and to combat illegal behaviours, Atlantia has already adopted the "Compliance Programme for Atlantia's foreign subsidiaries" (the "Compliance Programme" or "CP").

In order to harmonize existing set of rules among its foreign subsidiaries ("Foreign Subsidiaries" or "FS") in delivering a shared, consistent and global approach against illicit behaviours, Atlantia intends to hereby strenghten the Compliance Programme.

This initiative was undertaken with the firm belief that the adoption of the Compliance Programme constitutes a valid awareness-enhancement tool for all those operating in the name of ATLANTIA S.p.A. and/or its subsidiaries, so to ensure that they would behave in a professional and transparent way while performing their duties, thus avoiding the risk of offences being committed.

Where local laws and regulations contain mandatory requirements that differ from the provision of this CP, such mandatory requirements will prevail.

2. Purpose

This Compliance Programme represents an opportunity to reinforce a proactive prevention of corporate criminal liability by strengthening corporate governance and the overall internal control system and it is designed to support proper legal behaviours throughout the Group.

The Compliance Programme aims at building a structured and organic system for procedures and control activities to be carried out also pre-emptively (ex ante control), to prevent different types of offences.

In particular, the CP identifies the key standards of behaviour and control expected from all Corporate Recipients in order to:

- provide FS with a standard set of rules aimed at preventing a corporate criminal liability in their own country;

- integrate any local compliance program adopted by a FS in accordance to any applicable law on corporate criminal liability.

The rules contained in CP are integrated by:

- the provisions set out in the Code of Ethics, which represents the Group's ethical principles to which all Recipients are required to comply;
- the provisions set out in the Atlantia's Anticorruption Policy;
- the provisions of corporate governance adopted by FS, reflecting the applicable legislation and international best practice;
- the internal control system adopted by each FS.

In addition to the principles reported above, the Board of Directors of each FS is responsible for ensuring a suitable internal control systems for the prevention of the risk of corporate liability, according to local applicable regulations.

3. Adoption, Implementation and subsequent amendments

This version of Compliance Programme was approved by Atlantia on March 20, 2019. Any substantive change shall be approved by Atlantia.

Each FS shall adopt this CP in a timely manner by resolution of the Board of Director or the corresponding body or function.

The foreign ATLANTIA subsidiaries should respect the general instructions set out in this Compliance Programme, and any others guidelines issued by ATLANTIA in their regard.

The Board of Directors or the corresponding body or function of each FS, acting in their own autonomy and independence:

I. adopts the most appropriate measures for the implementation and monitoring of the CP, taking into account the organization, complexity of business, specific risk profile concerning the FS and its regulatory framework.

II. is responsible for approving any analyses for identification of Area at Risk, General Standards of Control and/or Key Standards of Behaviour, in addition to those identified in Sections 11 of the CP to be implemented through local internal procedures

The Chief Executive Officer and/or the Compliance Officer of each FS shall report to the Group Compliance Officer any changes, additions or not applicable parts in accordance with local legislation or customs and referring to current operating environment.

4. Roles and Responsibilities

Atlantia

Atlantia S.p.A. is responsible for approving and updating the Compliance Programme that contains the guidelines to be applied globally.

Board of Directors or other governing body of Foreign Subsidiaries

The Board of Directors or other governing body of Foreign Subsidiaries is responsible for:

- adopting the Compliance Programme approved by Atlantia or communicating to Atlantia the reasons for not adopting it fully or partially ;
- approving the results of internal analyses aiming at adding or modifying the areas at risk to be monitored with regard to local regulation as well;
- identification and appointment of the structure (FS Compliance Officer) in charge of providing support in the monitoring of CP.

The Board will appoint as FS Compliance Officer, the Chief Executive Officer (CEO) or the Managing Director or other Manager.

FS Compliance Officer

The FS Compliance Officer has the responsibility to apply and continuously verify the compliance with the general principles and instructions contained in this Compliance Programme.

Moreover, with regard to local law and regulatory requirements, the FS Compliance Officer has the task of:

- supervising the updating of this Compliance Programme;
- identifying further areas at risk.

He is responsible for communicating to the Group Compliance Officer the results of the risk analysis carried out at the local level, as well as any changes to the Compliance Programme applied locally.

Group Compliance Officer and General Counsel

The Group Compliance Officer, jointly Atlantia's General Counsel shall constantly monitor regulations and case law regarding corporate liability.

In addition, the Group Compliance Officer shall be informed about the results of the risk analysis carried out at the local level and the results of the monitoring on the compliance programme in order to propose any updates thereof introduced locally.

Internal Audit Department

As part of its monitoring activities on foreign subsidiaries, the Group Internal Audit department will also perform the activities required to ensure compliance with the provisions of this Compliance Programme on the basis of its own annual auditing programme approved by the Board of Directors of Atlantia.

The Group Internal Audit department can also perform spot audits based on specific requests that may occur (e.g. reporting of Compliance Programme violations).

Training and Communication

Foreign Subsidiaries shall ensure awareness of the Compliance Programme, the Code of Ethics and the Anticorruption Rules and Regulations by all staff.

Each Foreign subsidiary shall plan and manage training activities on the contents of this Compliance Programme.

The training should provide practical examples of how crimes could be committed within each Area at Risk, how to deal with suspicious behaviours, instructions to recognize "red flags" and avoid questionable actions for the purpose of this CP.

Participation in training activities is mandatory. The Human Resources Departments of the Foreign Subsidiaries shall ensure that all personnel follow the planned training programme.

The principles and contents of this CP, which are also applicable to Third Parties, are brought to their attention through proper contractual documentation, which shall provide for standard clauses that, based on the activity regulated by the contract, shall bind the counterpart to comply with the CP's Key Standards of Behaviour directly applicable to them.

5. Internal Reporting System

Each Corporate Recipient shall report to the FS Compliance Officer any suspected violation of this Compliance Programme by using the dedicated e-mail address [complianceofficer@companydomain].
In case of violation or suspected violation of Anticorruption Rules, a notification should also be sent to the Anticorruption Officer via the dedicated e-mail address [anticorruption@companydomain]
When contacted by the FS Compliance Officer, each Corporate Recipient shall be obliged to cooperate with investigations relating to the alleged misconduct. Failure to cooperate and provide honest, truthful information could result in disciplinary action.
Furthermore, the FS Compliance officer shall report every year to the Board on the activities performed in connection with the application of this Compliance Programme
Atlantia and each FS will not tolerate any retaliation against anyone who, in good faith, reports a concern or cooperates with an investigation. Directors or employees who retaliate against any other employee will be subject to disciplinary action, up to and including termination for cause, in accordance with applicable laws. Any suspected retaliation should be reported immediately. Each Foreign Subsidiary shall take any proper measure to grant confidentiality.
Certainly, the rights and obligations of reporting to the competent public authorities remain subject to the requirements of the local laws.

6. Disciplinary System and contractual remedies

Violations of laws on criminal or quasi-criminal liabilities of corporate entities can cause criminal, civil and regulatory penalties, including fines and jail, as well as a damage to the Group's reputation.
Proper disciplinary measures shall be applied by the competent FS' function in the event of breach of any Key Standard of Behaviour set out in the CP, in accordance with the disciplinary system already in force, pursuant to applicable rules or local compliance programmes and without prejudice for the protection afforded to employees under local legislation. The Group Companies will also fully cooperate with the Authorities.
Each Foreign Subsidiary will take appropriate measures, including but not limited to contract termination, against Third Parties whose actions are found to be in violation of those Key Standards of Behaviour applicable to the latter.

7. Monitoring

Every Foreign Subsidiary shall guarantee that its own crimes prevention management system meets the general requirements and is committed to improving such system on an ongoing basis.

The task of monitoring the operation and observance of the Compliance Programme is entrusted to the FS Compliance Officer. The objective of the execution of any supervisory action is to evaluate the adequacy and effective operability of the control actions required by section 11 of this Compliance Programme

The FS Compliance Officer has the responsibility of reporting every year to the corresponding Board of Directors on the activities performed in connection with the application of this Compliance Programme.
Moreover, the FS Compliance Officer and the Group Compliance Officer may recommend improvements to the Compliance Programme on the basis of any newly introduced best practices.

The Internal Audit department, throughout the monitoring activities on Foreign Subsidiary, shall review and assess the internal control system to ensure that the provisions of the Compliance Programme are applied.

In case of violations (both violations of local rules and violations of general behaviour and control standards), the FS Compliance Officer and the Group Compliance Officer , with support from the Internal Audit department, will consider whether any revisions or amendments to the Compliance Programme might help to prevent the recurrence of the violation.

8. Crimes

The Compliance Programme applies to the following types of crimes:

1. Corruption crimes
2. Other crimes against Public Entities
3. Accounting Fraud
4. Financing of Terrorism and Money Laundering crimes
5. Market Abuse
6. Crimes against Individuals
7. Health and Safety crimes
8. Environmental crimes
9. Cyber crimes
10. Copyrights crimes

Section 11 below identifies the areas of activity to be monitored by FS and the applicable key standard of behaviour and control.
The list included in paragraph 11 does not exempt Foreign Subsidiaries from carrying out their own risk assessment and definition of key standards of behaviour and control if deemed appropriate.
Therefore, each FS might identify:

- the business activities which may entail specific risk of committing a crime through an analysis of business processes and the possible ways of commission attributable to the types of offences;
- additional standards of behaviour which all Corporate Recipients and – where expressly specified – Other Recipients have to deal with in order to:
    - refrain from any behaviour that gives rise to any of the crimes described above;

- refrain from any behaviour that, even though does not constitute in itself as any of the crimes listed above, could potentially lead to the latter.

9. General Standards of control

To comply with the Compliance Programme, the Foreign Companies shall adopt and abide by the following general standards of control.

Segregation of duties:

The party performing an operational activity must be different from the party that controls such activity (and/or the party that authorises it, where applicable), as operational activities and control functions need to be adequately segregated; an adequate segregation of duties can be granted also using IT systems enabling only identified and authorized persons to perform certain transactions;

Powers of signature:

Power of signature must be adequately formalised and clearly defined and be attributed in close connection with the needs associated with the specific organisational and management responsibilities of the executive vested with them. Powers of signature shall be consistent with the organizational and managerial responsibilities assigned to each proxy holder within the FS.

Traceability and storage:

All the activities carried out and the relevant controls performed must be traceable and verifiable ex post. The documentation produced must be filed properly and be easily retrievable; proper storage of data and relevant information must be guaranteed, through information systems and /or paper support.

Proper management of Third Parties' relationships:

All process owners must implement, within the scope of their duties and responsibilities, proper procedures (in accordance with reasonableness and proportionality criteria with respect to the relationship to be established):

(i) to check the reliability, reputation and adequacy of any third party with whom each Foreign Subsidiary is considering the establishment of a professional and business relationship; the extent of each due diligence assessment shall be proportional to the actual or perceived risk that any prospective partner, consultant or supplier can be not in possession of the above mentioned requirements;

(ii) to lay down specific contractual provisions that require third parties to comply with the principles contained in the Code of Ethics and in this Compliance Programme;

(iii) to check the effectiveness of the services rendered by third parties in pursuance of the contracts entered into with Group Companies and determine the reasons for the payments as well as the fairness of the amounts to be disbursed.

Each Foreign Subsidiary shall guarantee that the Compliance Programme will also be made known to its commercial and financial partners, professionals, consultants, commercial promoters, all types of collaborators and suppliers.
Such parties shall be required to sign a statement confirming that they have knowledge of the CP and that they undertake to comply with it and ensure that their assignees or successors and contracting parties shall comply with it.

10. Areas at Risk and Key standards of behaviour and control

A. Corruption crimes

Corruption crimes are the product of certain behaviours whereby anybody who, acting directly or indirectly on behalf or in the interest of Group Companies, offers, promises, receives or provides undue rewards and/or compensation and/or other advantage, directly or indirectly (thus through third parties), for personal benefit, and/or for the benefit of Group Companies or third parties. For the purposes of the Compliance Programme, there is no difference between “corruption of a Public Official or a Person Performing Public Services” and “corruption of a private party”; therefore the provisions of this Compliance Programme must be respected even in private-to-private relations, also where not expressly indicated from time to time.

Trading of influence occurs when a person who has real or apparent influence on the decision-making of a public official (or on other decision maker) exchanges this influence for money or other advantage as compensation for the unlawful mediation.
Trading of influence is the illegal practice of using one's influence in government or connections with persons in authority to obtain favours or preferential treatment for another, usually in return for payment or other advantage.
It is also an offence for any person to give or promise money or other advantage in exchange for unlawful mediation (real or apparent).

The offences of trading of influence and bribery have very similar elements, with one major exception. For the bribery offence, the briber must offer, promise or give the bribe with the intention that the bribed official act or refrain from acting in the exercise of his/her functions or duties, etc. For trading of influence, the briber must intend that the recipient of the bribe influences the decision-making process.

This offences often take the form of gifts or payments of money (other forms of corruption may include various goods, privileges, advantages, entertainments and favours) in exchange for favourable treatment, including the so-called facilitation payments.
Such favourable treatments, which represent the reasons for the briber to perpetrate such behaviour, may consist, for example, in:

- the engagement of the briber for a relevant contract;
- the awarding of a public tender;
- a false deposition, favourable to the briber, by a witness in a trial;
- a lenient report by a public official after an inspection.

AREAS AT RISK

In relation to this type of crimes, the following areas could be deemed to be at risk:

a) negotiation, execution and management of material contracts with any party (Public Authorities, companies, associations, foundations, etc.);
b) participation to public or private tenders;
c) dealings with Public Authorities (in all their ramifications);
d) management of disputes (lawsuits, arbitration, out-of-court proceedings);
e) selection of partners, intermediaries and consultants and negotiation, execution and management of the related contracts;
f) management of cash and financial resources;
g) acquisitions of equity stakes in other companies and joint ventures (M&A);
h) staff selection and recruitment;
i) management of non-profit initiatives and sponsorships;
j) management of gifts, entertainments and hospitality expenses;
k) reimbursement of expenses incurred by employees.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

In conducting business with private companies as well as public administrations, state and local governments, national, international and supranational institutional bodies (the "Public Authorities"), FS and their representatives are committed to act with integrity and honesty and shall comply with all applicable laws and regulations.

Key Standards of Behaviour applicable to Corporate Recipients are specifically set out in the Anticorruption Policy.

Moreover, within the framework of this Compliance Programme, all Company Representatives directly, and independent consultants and partners by means of specific agreement terms shall expressly refrain from:

a. making payments to public officials (deemed as any official, officer or employee of a government or any department, agency, or any person acting in an official capacity for, or on behalf of, said government or department or agency etc.);
b. giving gifts and gratuities except as per the company's customary practice; in particular, it is prohibited to offer any form of gift to public officials (including those countries where this is a widespread practice), or to their relatives, which may affect their impartiality of judgment or induce them to grant an advantage of any kind to the company. Permitted gifts shall always be either reasonable and of modest value; they must not take the form of cash or a cash equivalent;
c. according other advantages of any kind (e.g. promises to hire etc.) to Public Administration representatives, that may lead to the consequences described in paragraph b) above;
d. rendering services in favour of partners that are not justified within the framework of the partnership agreement established with those partners;
e. paying to independent consultants fees that are not justified compared to the assignment they have to perform and to common local practices.

The following principles shall apply for the purpose of implementing the Standard of behaviour described above:

- adequate evidence shall be given as to all principal relations with Public Administrations regarding “at-risk activities”;
- all partnership agreements shall be defined in writing, specifying the terms of agreement, relative to the financial terms for joint bidding;
- all assignments given to independent consultants shall also be made in writing, specifying the fees agreed and the object of the contract; proper evidence of the fee calculations and of the work performed should be recorded by the Company;
- consultants or other Third parties working for or on behalf of Atlantia or one of its subsidiaries must sign a provision of no conflict of interest existence and must operate within the rules and ethical principles of the Code of Ethics. Any breaches in the Code of Ethic should result in the cancellation of the assignment;
- no payment in cash shall be allowed;
- all managers and supervisors in charge of the obligations related to the performance of these activities (payment of invoices, allocation of State or European Community funds etc.) shall comply with said obligations and report immediately any irregularity to the Managing Director;
- within the company, suitable evaluation systems might be put in place for the selection of agents, consultants etc., as well as partners with whom the Foreign Company intends to make a partnership (e.g. a joint-venture, also in the form of a temporary company association or consortium etc.), and be used to cooperate with the company in the performance of “at-risk activities”;
- any behaviour by agents or consultants etc., as well as partners with whom the Foreign Company intends to make a partnership, which contrasts with the Guidelines of behaviour stated in this document, might result, according to the provisions contained in the specific clauses of the job orders or in the partnership agreements, in cancellation of the agreement subject to the possibility of the company applying for damages if such behaviour causes real damage to the company.

Furthermore, FS shall adopt adequate procedures in order to ensure that:

- the authority and necessary powers to make contact with the public administration are formalised and defined;
- adequate evidence is given in relation to any material relationships (e.g. administrative proceedings aiming at obtaining an authorization, a license or similar act, joint ventures with public entities) entered with Public Authorities;
- relationships with Public Authorities and Third Parties are managed by at least two authorized persons;
- all Third Parties’ agreements are entered in writing specifying all the terms of agreement, even if the written form is not strictly required by applicable law, and that prior to paying the related invoices, the FS can verify the effectiveness, quality, consistency and timeliness of the performance received by the Third Party and the fulfilment of all obligations undertaken by the latter;
- any recruitment procedure is carried out solely on the basis of a real and demonstrable business need, the selection process involves at least two functions and is based on criteria of competence and professionalism aimed at avoiding favouritism or nepotism;

- in relation to expense reimbursements, proper documentation, including original receipts supporting the payment of the expenses or incurring the cost, shall be submitted to the appropriate accounting department before payment and proper registration of the payment in the relevant books and records.

B. Other crimes against Public Entities

This type of crimes mainly relates to fraud against public entities and occurs when a company executes one or more actions or illicit schemes in order to defraud a public entity to obtain any economic advantage through false or fraudulent representations, promises or pretences.

Such type of crimes are often connected to public funding, grants and tenders and occurs when a company claims for public funding or grants that it is not eligible for or misuse them in a manner different than outlined in the grant agreement.

This type of crime can take place for a number of reasons, which are normally related to obtaining of any economic advantage.

AREAS AT RISK

In relation to this type of crimes, the following areas should be closely monitored:

a) participation to public tenders and public works in general;
b) application for public funding, grants, subsidies or guarantees issued by Public Authorities;
c) management of the received public funding, grants subsidies or guarantees obtained.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

In addition to key standards of behaviour set out in paragraph 11 letter A) above, Corporate Recipients shall refrain from:

- submit untrue statements to government or Community public authorities in order to obtain public funds, grants or facilitated loans;
- allocate amounts received from State or Community public authorities as funds, grants or loans for other purposes than those they were intended for;
- carry out cheating behaviours against the Public Authorities, which may induce the latter to make a wrongful assessment during the examination of requests for authorizations, licenses, clearances, concessions, etc.

Furthermore, in order to implement the behavioural standards described above, the Foreign Companies are required to adopt proper organizational measures in order to ensure that:

- all the statements rendered to national or international public authorities for the purpose of obtaining funds, grants or loans contain only true information and be signed by authorized signatories and, where said funds, grants or loans are obtained, these are appropriately accounted for;
- request, management and reporting phases in relation to public proceedings for the purpose of obtaining funds, grants or loans are managed by different Corporate Recipients within the organization;

- the activities of collecting and analysing the information which are necessary for reporting purposes are carried out with the support of the competent functions;
- the documentation and the subsequent reporting to be submitted in relation to the request of subsidies, grants, loans and guarantees need are approved by adequate hierarchical levels.

In addition, the formalization of the following documents must be guaranteed:

- the letter to request public financings and contributions and related powers of attorney;
- the related contract;
- the payment certificate, invoice or any supporting documents related to the financings and contributions granted.

C. Accounting Fraud

Accounting fraud is intentional manipulation of financial statements to create a facade of a company's financial health. It involves an employee, account or the organization itself and is misleading to investors, shareholders, stakeholders and auditors. A company can falsify its financial statements by overstating its revenue or assets, not recording expenses and under-recording liabilities.

Accounting fraud can take place for a number of reasons, including but not limited to:

- keep obtaining financing from a bank;
- report unrealistic profits or hide losses;
- hide circumstances which could affect negatively the company;
- disguise the creation of slush funds.

AREAS AT RISK

In relation to this type of crimes, the following areas should be closely monitored:

a) drafting documents to be released to shareholders or to the public (e.g. financial statements, periodic financial reporting) regarding the assets and liabilities, revenues and expenses or cash flows of the Foreign Subsidiaries, even if such documents are other than the periodical accounting ones;
b) management of relationships with the external auditors.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

Regarding the areas at risk identified above the Foreign Companies shall:

- conduct themselves diligently, transparently and cooperatively in accordance with the law and internal corporate procedures, all activities involving the preparation of financial statements and other corporate communications, in order to provide shareholders and others with true and accurate information concerning the economic, financial and balance sheet position of the company and its subsidiaries;
- comply rigorously with all provisions of law concerning maintenance of capital so as not to prejudice the rights of creditors and others in general;
- ensure the regular operation of the Company and Corporate Officers, guaranteeing and facilitating all forms of internal control of company management prescribed by law, as well as the free and proper expression of the will of the shareholders meeting;

- send all communications required by law and regulations to the relevant supervisory authorities promptly, diligently and in good faith, without obstructing the exercise of such authorities' supervisory duties in any way;

In addition, the Foreign Companies are required to:

- keep books, records and accounts which, in reasonable detail, accurately and fairly reflect the transaction and dispositions of the assets of the companies;
- design and maintain a system of internal control sufficient to provide reasonable assurance that:
    - transactions are executed in accordance with a management's general or specific authorisations;
    - transactions are recorded as necessary:
        a) to permit the preparation of financial statements in conformity with the generally accepted applicable accounting principles or any other criteria applicable to such statements, and
        b) to maintain the accounting for assets;
    - access to assets shall only be permitted in accordance with the management's general or specific authorisation, and the recorded accounting for assets shall be compared with the existing assets at reasonable intervals, and appropriate action shall be taken with respect to any differences.

Personnel assigned to keep books, records and accounts are required to act properly to ensure that:

- data and information used for the preparation of periodic financial reporting are accurate and diligently verified;
- all balance items, whose determination and quantification entail discretional valuations, are objective and supported by appropriate documentation;
- transactions are executed in accordance with the management's general or specific authorizations;
- invoices and other relevant documentation related to the transactions are properly vetted, recorded and stored;
- transactions are recorded as necessary to permit the preparation of financial statements in conformity with the applicable or generally accepted accounting principles or any other criteria applicable to such statements;
- access to such transactions records is allowed only in accordance with management's general or specific authorizations.

Furthermore, the Foreign Companies must refrain from performing any conduct that impedes or, in any case, obstructs the checking and auditing activities by the external auditors through the concealment of documentation or the use of other fraudulent means.

D. Financing of Terrorism and Money Laundering crimes

Financing of terrorism means the provision or collection of funds, by any means, directly or indirectly, with the intention to use them to support terrorist acts or organizations.

The primary goal of individuals or entities involved in the financing of terrorism is to conceal both the financing and the nature of the financed activity.

Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origin. More precisely, it may encompass three different behaviours: (i) the conversion or transfer of funds, knowing that they derive from illicit activities (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of a crime; and (iii) the acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of a crime.

When the proceeds of a crime are created by the same person concealing their illicit origin, such a conduct is punished in certain countries as self-money laundering.

Money laundering and financing of terrorism often display similar transactional features, mostly having to do with concealment.

Money launderers send illicit funds through legal channels to conceal their criminal origins, while those who finance terrorism transfer funds that may be legal or illicit in origin in such a way as to conceal their source and ultimate use, which is the support of terrorism.

These types of behaviours can take place for the benefit of a company for a number of reasons, including but not limited to:

- obtain proceeds or any other advantage arising from illegal activities carried out by the terroristic organizations which have been financed (the other advantages may consist in protection of the business, in countries where such organizations are rather influential);
- disguise the illegal origin of criminal proceeds.

AREAS AT RISK

In relation to this type of crimes, the following areas could be deemed to be at risk:

a) contractual relationships with suppliers, partners and other legal entities controlled directly or indirectly by the above-mentioned subjects – having their residence or a registered office in a country representing a high-risk and non-cooperative jurisdiction;
b) financial flows management.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

Foreign Subsidiaries shall condemn the use of its resources for the financing or execution of any activity aimed at reaching objectives associated with the financing of terrorism as well as any misuse of financial instrument and/or operation aimed at concealing the source of company's funds.

More generally, FS shall condemn any possible conduct aimed at, even indirectly, facilitating offences such as receiving, laundering and use of money, goods or any other utility of unlawful origin; in this regard FS is committed to implement all the requested preventive and subsequent control activities necessary to achieve that goal, regulating also relations with third parties by means of contractual provisions requiring the observance of the applicable laws on the matter.

In particular, it is specifically forbidden to:

- make or receive blank payments or cash for any operation of collection, payment, funds transfer, et cetera;
- issue or receive invoices or release documents in relation to non-existent transactions.

Furthermore, in order to implement the behavioural standards described above, the FS must:

- perform analytical controls of the cash flows;
- verify the validity of payments, by controlling that its beneficiary actually is the counterparty involved in the transaction;
- carry out procedural controls, in particular regarding possible transactions occurring outside the normal Company processes;
- retain evidence of all of the transactions carried out;
- ensure the traceability of every financial operation, as well as agreement or any other investment or business project;
- verify the economic consistency of such operations and investments;
- always check the international black list regarding terrorism and tax havens.

E. Market abuse

The Market Abuse crimes might refer to four different patterns of behaviour: (a) the purchase or sell of financial instruments, performed using information which is not publicly available ("Inside Information") (b) the illegitimate communication of such information to third parties; (c) the alteration of the price-setting mechanism of financial instruments by spreading false or misleading information or through simulated transactions or other artifices[1]; (d) the execution of purchase or sell orders which cause or are aimed at causing (i) the spread of false or misleading indications with regard to the offer, demand or price of financial instruments, (ii) the setting of the price of one or more financial instruments at an anomalous or artificial level, higher or lower than what the actual market price would be.

These types of behaviours can take place for the benefit of a company for a number of reasons, including but not limited to:

- deflate the share price of a target company before an acquisition;
- weaken the reputation of a competitor company;
- alter the price of a certain financial instrument in portfolio before carrying out any trading activity relating to it.

AREAS AT RISK

In relation to this type of crimes, the following activities could be deemed to be at risk:

a) management of public information, such as the information provided to investors, financial analysts, rating agencies and mass media, as well as the organization and participation in meetings with the aforesaid persons;
b) management of Inside Information connected to listed companies and, particularly, listed companies of the Group and relevant financial instruments;
c) drafting of companies' prospectuses and financial statements;
d) any kind of transactions relating to financial instruments in portfolio.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

[1] "Other artifices" means any behavior that, by deception, is suitable to alter the price-setting mechanism of financial instruments (e.g. the omission of unfavourable information that the market was required to know)

Each Recipient is expressly required to refrain from:

- using Inside Information to negotiate, directly or indirectly, financial instruments to obtain personal advantage, or to favour Third Parties or a FS or any other Group company;
- disclosing Inside Information to Third Parties, except when this is required by law, or other regulatory provisions or specific contracts in which the counter-parts are obliged to use the information only for the purpose originally intended and maintaining its confidentiality;
- recommending or inducing anybody, on the basis of certain Inside Information, to perform transactions on financial instruments;
- spreading false or misleading information (whether about the FS or about any other companies) through the media, the Internet, performing simulated transaction or other artifices, in order to alter the market price of financial instruments;
- performing any transactions on financial instruments against the market abuse regulations.

F. Crimes against Individuals

The crimes against Individuals are those offences referring to forced labour practices (mainly consisting in coercing individuals to work through the use of violence or intimidation, or by other means such as retention of identity papers) or to exploitation of the workers.

Such crimes could be committed when Foreign Subsidiaries:

- exploit a worker taking advantage of his/her situation of physical or psychological state of need;
- compel individuals to work, using threats, abuse of authority and/or violence;
- compel immigrant individuals to work under threat of denunciation to immigration authorities.

This type of crimes can be committed for a number of reasons, such as:

- employ a workforce with minimal compensation;
- employ a fully subservient workforce, to which no request would be refused.

In addition, within the crimes against individuals may be included all actions that violate the respect for people and human rights in all their forms, including ethnic, cultural, racial and religious differences (e.g. propaganda or incitement of crimes of genocide, crimes against humanity and war crimes, incitement to discrimination or violence on racial, ethnic, national or religious grounds).

AREAS AT RISK

In relation to this type of crimes, the following should be considered at risk areas:

a) recruitment;
b) entering into contracts with suppliers that utilize unskilled personnel;
c) entering into partnerships with local suppliers in countries where individual rights are not fully protected by legislation;
d) dissemination of advertising content also on behalf of third parties.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

The Foreign Subsidiaries are required to:

- select external Third Parties (e.g. partners, suppliers, sponsees, tenants) – especially those providing for non-technical services – only after having accurately verified their reliability;

- execute proper contractual documentation with external contractors requiring them to comply, and requiring their subcontractors to comply, with any applicable international and local legislation (e.g. ILO conventions on the minimum age for employment and on the worst forms of child labour) on forced labour, protection of child labour and of women and compliance hygienic-sanitary conditions;
- implement and enforce any contractual penalties in the relevant agreement in the event of breach by a contractor or any of its subcontractors of any international or local legislation applicable;
- ensure the utmost respect for people and human rights in all their forms, including respect for ethnic, cultural, racial and religious differences;
- implement a formalized human resources hiring process.

In addition, it is specifically forbidden to:

- approve advertising contents that instigate or incite, so that it derives concrete danger of diffusion, to racism and / or xenophobia;
- facilitate in any way the dissemination of advertising or promotional messages that promote, even implicitly, racism and xenophobia;
- authorize the sale or lease of Company's assets to entities aimed at prosecuting the spread of racism and / or xenophobia.

G. Health and Safety crimes

Health and safety crimes are mainly related to the non- compliance with local legislations and labour standards to be granted in the workplace in order to avoid employees' accidents and illnesses.

These types of behaviours can take place for the benefit of a company for a number of reasons, including but not limited to:

- the reduction of costs, for the adoption of the required measures often entails additional expenses for a company;
- the increase of productivity, given that working without taking into account precautionary procedures and policies might speed up the work processes.

AREAS AT RISK

In relation to this type of crimes, the following areas have to be regarded as at risk:

a) compliance with applicable health and safety laws.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

Regardless of the wideness of local legislation addressing health and safety in the workplace, FS shall introduce an occupational health and safety management system, to enable the company to control its health and safety at work risks and develop a proper internal control environment to prevent all the risks related to labour law violations (according to the applicable labour laws in the specific country).

Foreign Subsidiaries shall always take into account the safety of workers, throughout any phase of the activity and shall commit to adopt all the measures that are deemed necessary to protect its workers' physical and moral integrity.

In particular, FS shall:

- consider the compliance to the provisions of law governing the health and safety of workers on the workplace as a priority;
- as far as possible and allowed by the best techniques' evolution, evaluate the risks for workers with the aim of protection, also by adopting the most adequate and safe materials and equipment, in order to reduce the risk at the source;
- correctly evaluate those risks which are not avoidable and adequately mitigate them by implementing appropriate individual and collective safety measures;
- disseminate information regarding health and safety in the workplace, up to date and specific with reference to the activity performed, ensuring that workers are properly trained;
- grant that management incentive plans are adopted in a way to ensure that the objectives set thereto are such as not to lead to abusive behaviour and are focused on a well determined and measurable outcome;
- timely consider and analyse any non-compliance or improvement area, emerged during the working activity or during inspections;
- set the organization of the working activity in order to protect the integrity of workers, Third Parties and the community within which the FS operates.

In order to keep properly monitoring the Areas at Risk, each Foreign Company assigns organizational, instrumental and economic resources to ensure, on the one hand, full compliance with the current provisions of law on workplace accidents prevention and, on the other hand, the continuous improvement of workplace health and safety situation, also by means of implementation and updating of the relevant preventive measures.

Corporate Recipients must cooperate in order to grant the full respect of the provisions of law, corporate procedures and of any other internal regulation aimed at protecting the safety and health of workers in the workplace.

H. Environmental crimes

An environmental crime is a violation of environmental laws that are in place to protect the environment. When broadly defined, the crime includes all illegal acts that directly cause environmental harm. Such crimes are related to a broad list of illicit activities, such as crimes against wildlife, illicit trade and disposal of hazardous waste substances and many other acts that could harm the environment.

Environmental crimes usually affect the quality of air, water and soil, threaten the survival of species, may cause uncontrollable disasters and might cause a security and safety threat to a large number of people.

For example, Environmental crimes could take place if someone within a company:

- does not consider the local fauna when planning the activities to be performed and selecting the physical areas in which to operate, thus harming the habitat of protected animal species and jeopardizing their existence;
- does not properly performing Company's waste disposal activities by setting up an illicit waste disposal site.

These types of behaviour can be committed in the interest of a company for a number of reasons, including but not limited to:

- reduce costs, since the adoption of the measures needed to safeguard the environment often entails additional expenses;
- increase productivity, given that working without considering the environmental issues might speed up the production process.

AREAS AT RISK

In relation to this type of crimes, the following areas should be closely monitored since they are considered as at risk:

a) compliance with applicable environmental laws in connection with the design, construction, management and maintenance of plants and related infrastructures.
b) selection of the Third Parties that have to perform specific activities that can affect the environment (e.g. waste management and disposal).

KEY STANDARDS OF BEHAVIOUR AND CONTROL

In its business, each Foreign Company shall consider the respect and protection of the environment as a priority and, in particular, it shall

- disseminate within the Company information regarding environmental protection, promoting awareness to such issue and ensuring that the activities are performed in compliance with relevant applicable legislation;
- adopt the appropriate instruments in order to prevent its activities to cause any form of damage and harm to the ecosystem;
- set forth in the agreements with the Third Parties where Company's liability under environmental law may arise, specific and enforceable contractual penalties in case of breach, by a contractor or any of its subcontractors, of any applicable international or local legislation addressing the issue in question;

I. Cyber crimes

Cyber crime refers to any crime that involves a computer and a network. Computer crime encompasses a broad range of activities. Generally, however, it may be divided into two categories: (i) crimes that target computers and devices; (ii) crimes facilitated by computer networks or devices.

Cyber crime consist, for example, in: (i) unauthorized intrusion into a protected network; (ii) introducing of computer viruses into a protected network; (iii) interception of data from a computer network. For instance, Cyber crimes could be committed by someone within a company in the event that they:

- install an illegally copied software on work devices;
- enter a competitor company's computer system by hacking it;
- introduce a virus into a competitor's computer system;
- hack a competitor's computer system in order to be always able to have access to its content.

Cyber crimes can take place for a number of reasons, such as:

- to access a competitor company's business secret;
- to obtain confidential information about competitor companies' market strategies;

- to jeopardize or damage a competitor company's computer system;
- to use, without authorization, a protected computer program, illegally reproduced.

AREAS AT RISK

In relation to this type of crimes, the following must be regarded as at risk areas:

a) company activities performed by using the Company Intranet, Internet, the electronic mail system or any other IT instrument;
b) management and protection of workstations, laptops, mobiles and storage devices;
c) planning of the measures to be adopted on electronic system as well as security, classification and processing of information and data.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

Each Recipient shall refrain from carrying out the following behaviours:

- improper use of IT credentials;
- unauthorized sharing of business information outside of the Company and the using of personal or unauthorized devices to transmit or store company information or data;
- tampering or alteration of the Foreign Company computer systems;
- exploitation of any gaps in the security measures of corporate IT systems to gain access to the information without proper authorization;
- unauthorized installation of software and databases;
- use of unauthorized software and/or hardware that could be used to compromise the security of IT systems (such as software to identify the credentials, decrypt encrypted files, etc.).

FS shall ensure a periodical monitoring, in compliance with local applicable law, on the activities performed on the corporate IT system by the personnel, in order to detect unusual behaviour and potential vulnerabilities in corporate systems.

Furthermore, the Foreign Companies shall increase, also through specific training sessions where needed, the personnel's awareness about the importance of a correct and proper use of the IT tools in their possession.

With regard to the use and management of systems, tools, documents or computer data, all Corporate Recipients must comply with the following principles of control:

- compliance with the procedures for managing IT security;
- preparation and implementation of a company policy for the management and control of physical security of the environments and resources;
- adoption of specific measures to guarantee the separation of roles in the change management process (new developments, evolutionary maintenance, corrective maintenance and ordinary maintenance) of IT systems (application software or basic software, hardware and systems);
- prediction and implementation of processes and mechanisms of disaster recovery that guarantee the restoration of certain systems and data in case of temporary unavailability or permanent loss;
- adoption of specific measures to guarantee that the use of assets possibly covered by intellectual property rights in accordance with legal or contractual provisions;

- use of the applications relating to customer data submitted to IT logs, in order to control any behaviour implemented by authorized users that is not in line or is forbidden by internal/external regulations;
- implementation of a protection system suitable for identifying and authenticating users that have been previously authorized and who wish to obtain access to a processing or transmission system;
- preparation of technological tools and levels of protection against spam, spyware, and malware prevent and/or prevent the creation of computer crimes;
- activation of filters suitable to prevent access to sites not related to work activities or forbidden;
- withdrawal of authorization to use an IT system/application at the end of the employment relationship, a change of corporate role or as a consequence of non-use for a prolonged period.

J. Copyrights crimes

Copyrights crime is the use of works protected by copyright law without permission, infringing certain exclusive rights granted to the copyright holder, such as the right to reproduce, distribute, display or perform the protected work, or to make derivative works.

For the purpose of CP, crimes against Copyrights mainly refer to illicit use of software and databases. This type of crimes can take place for a number of reasons, such as the reduction of costs, by refraining from paying for software licenses.

AREAS AT RISK

In relation to this type of crimes, the following areas need to be monitored:

a) company activities carried out by Recipients by means of Intranet and any IT tool provided or made available by the FS.

KEY STANDARDS OF BEHAVIOUR AND CONTROL

The Foreign Subsidiaries shall evaluate the opportunity to adopt proper technical, physical and organizational measures in order to avoid:

- any illegal use or dissemination to the public, through computer based networks or through connections of any other type, of protected original work, or any part thereof;
- use, distribution, extraction, sale or lease of the contents of a database breaching the exclusive right of execution and authorisation from the copyright holder;
- illegal download of any software without the execution of any proper contractual documentation;
- the downloading of peer-to-peer software or any other software not directly connected to the corporate activity.

When a Foreign Company stipulate a contract with external contractors for the performance of activities that could potentially be regarded as at risk of violating any copyright/proprietary rights, such contract must set forth provisions by means of which the contractor commits to comply with applicable laws and regulations.