Global Compliance Guidelines

Issue date: November 13, 2018

Table of Contents

1. SCOPE OF APPLICATION

Geox S.p.A. ("**GEOX**") is an Italian company, listed on the Italian Stock Exchange, parent company of a multinational group operating in the creation, production, and distribution of Geox-brand footwear and apparel, the main feature of which is the use of innovative and technological solutions that can guarantee the ability to breathe and remain waterproof at the same time (the "**Group**").

1.1. ITALIAN LEGISLATIVE DECREE 231/2001 AND GEOX 231 MODEL

The Italian Legislative Decree 231/2001 (the "**Decree**" or "**231 Decree**") introduced in Italy the concept of the corporate criminal liability of legal entities (companies; associations; etc.).

Specifically, pursuant to the Decree, a regime of responsibility has been introduced in the Italian legal system against companies and other entities for particular crimes committed in their interest or advantage by their managers and employees or by subjects subordinated to their direction or vigilance (e.g. consultants, agents, etc.). This responsibility is in addition to that of the individual who has committed the crime.

The liability provided for in the Decree applies in relation to the commission of numerous crimes, among which, the principal types of crimes are the following:

- Bribery and private-to-private bribery
- Fraud and other crimes against public authorities
- Accounting fraud
- Financing of terrorism
- Money laundering crimes
- Market abuse crimes (e.g. insider trading and market manipulation)
- Crimes against individuals (e.g. labor exploitation)
- Crimes that arise from failure to take care of health, safety and welfare at work
- Environmental crimes
- Cyber crimes
- Intellectual property crimes.

Among the sanctions provided by the Decree, the most severe include penalties up to Euro 4.5 million (up to Euro 75 million for market abuse crimes) and disqualifying measures such as the suspension or revocation of licenses and concessions, the prohibition to contract with government and public agencies, the

suspension of business activities, the exclusion or revocation of loans or contributions and the prohibition from advertising goods and services.

By introducing the above-mentioned liability system, however, the Decree provides for a specific exemption from this liability provided that the company:

- prior to the crime committed, adopted - and effectively implemented – a compliance program that was suitable for preventing crimes similar to that committed (so called "231 Model" "*Modello 231*");
- the task of supervising the implementation of the 231 Model, as well as its updating, was entrusted to a supervisory board ("*Organismo di Vigilanza*"), having independent initiative and control powers;
- the person(s) who committed the crime fraudulently avoided compliance with the above-mentioned 231 Model;
- the supervisory board didn't fail to supervise, nor the supervision was insufficient.

GEOX – being sensitive to the need of guaranteeing transparency and professionalism in conducting its business activity, of protecting its business position and image, its shareholders' expectations and its employees' jobs – deemed it consistent with its corporate policies to adopt and implement a 231 Model in compliance with the Decree (the "**Geox 231 Model**"). Geox 231 Model can be consulted on the following link: www.geox.biz/it/governance/regolamenti-procedure/modello-231.html

Geox 231 Model applies to all people acting in the name or on behalf of Geox (directors, managers, employees, consultants, etc.) and aims at building a structured and organic system of both procedures and control activities, to be carried out also preemptively (*ex ante* control), to prevent the different types of crimes envisaged by the Decree.

In particular, by identifying the business activities considered at risk with regard to the crimes included in the Decree (so called "Areas at Risk") and their consequent procedural definition, Geox 231 Model aims at:

- creating, in all the people who operate in the name or on behalf of GEOX in the "Areas at Risk", the awareness that, in case a crime is committed, it cloud give rise to criminal penalties both for the person committing the crime and the company;
- confirming that such illegal behaviors are strongly condemned by GEOX in that (even if the company appears to benefit from them) they are nevertheless against not only the legal provisions but also the ethical and

social principles GEOX intends to strictly comply with in pursuing its corporate mission;

- allowing GEOX, by monitoring the "Areas at Risk", to take action in a timely manner to prevent or oppose to such crimes;
- preventing risks, by adopting specific procedural principles in order to plan the company's decision-making process in connection to crimes to be avoided.

1.2. NON-ITALIAN COMPANIES AND GLOBAL COMPLIANCE GUIDELINES

In many of the foreign countries in which the Group operates (e.g. UK, Germany), a criminal or *quasi*-criminal corporate liability regime, similar to the one adopted in Italy through the Decree, has been established (mainly with reference to bribery crimes) which enables courts to sanction corporate entities for illicit behaviors by their representatives, employees or third parties acting on their behalf.

As done by the Decree, most of these regulations encourage companies to adopt corporate governance structures and risk prevention systems to make efforts to prevent these individuals from committing crimes, also providing for an exemption or mitigation of applicable penalties in the event of the adoption of adequate preventing measures.

That said, GEOX intends to adopt this global compliance guidelines (the "**Global Compliance Guidelines**" or "**GCG**") in order to harmonize existing efforts amongst the non-Italian companies of the Group (the "**Non-Italian Companies**" or the "**NIC**") in preventing criminal corporate liability and, more generally, illicit behaviors and to deliver a shared, consistent and global approach against them.

As well as to Geox 231 Model and to the Decree, the GCG has been inspired to the most relevant international regulations, including but not limited to:

(i) Good Practise Guidance on Internal Controls, Ethics, and Compliance adopted by OCSE on February 18, 2010

(ii) The 2010 Federal Sentencing Guidelines Manual & Supplement, released by the United States Sentencing Commission on November 1, 2010

(iii) Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide, UNODC, dated September 2013

(iv) UK Bribery Act 2010

(v) Recommendations adopted by the Financial Action Task Force (FATF) on Money Laundering and Financing of Terrorism

(vi) European regulations on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

(vii) Wolfsberg AML Principles.

The GCG aims at defining general standards of behaviour applicable to employees, directors and any other member of the management and control bodies of the NIC ("**Corporate Recipients**") as well as consultants or other contractors and, in general, third parties ("**Third Parties**" or "**Other Recipients**") (hereinafter the Corporate Recipients and the Other Recipients will be jointly referred to as the "**Recipients**") who are respectively employed or appointed or who deal with or act on behalf of the Non-Italian Companies.

More precisely, the GCG identifies the key standards of behaviour expected from all Corporate Recipients and – where specified – from Other Recipients in order to:

(i) provide NIC with a standard set of rules, aimed at preventing a corporate liability in their own country and in Italy;

(ii) integrate any local compliance program adopted by a NIC in accordance to any applicable law on corporate criminal liability.

The GCG is intended to be applied globally to all NIC in accordance with their legal and corporate governance as well as the cultural, social and economic differences in the various countries where they operate.

If local laws and regulations, or policies adopted by a NIC contain mandatory requirements that exceed the requirements of this GCG, such requirements will prevail.

2. GCG AND THE GROUP INTERNAL CONTROL SYSTEM

The rules contained in the GCG are integrated by:

(i) provisions set out in the Code of Ethics, which represents the Group's ethical principles to which all Recipients are required to comply;

(ii) provisions of corporate governance adopted by each NIC, reflecting the applicable legislation and international best practises;

(iii) internal control system adopted by each NIC;

(iv) provisions set out in any local compliance program adopted by each NIC to comply with their own local legislations on corporate liability and in any related guidelines, policy or internal organizational documents.

3. GCG'S STRUCTURE

The GCG identifies:

(i) adoption, update and improving processes to be implemented by each NIC;

(ii) training and communication to Recipients;

(iii) disciplinary system and contractual measures applicable in the event of breach of any provision contained therein;

(iv) general standards of control (the "**General Standards of Control**");

(v) areas at risk to be monitored (the "**Areas at Risk**") in relation to certain types of illicit behaviors - as listed in Section 8 - which are broadly considered crimes, might be potentially committed by a Corporate Recipient or a Third Party and the prevention of which GEOX considers to be a priority to run its business with honesty and integrity (the "**Crimes**");

(vi) key standards of behavior connected to the Areas at Risk (the "**Key Standards of Behaviour**").

4. ADOPTION, IMPLEMENTATION AND SUBSEQUENT AMENDMENTS; LOCAL COMPLIANCE OFFICER AND GLOBAL COMPLIANCE OFFICER

The GCG has been approved by the Board of Directors of GEOX on November 13, 2018.

Each NIC shall adopt this GCG in a timely manner by resolution of the board of director or the corresponding body or function.

Further substantive changes and additions to the GCG shall be entrusted to the Board of Directors of GEOX and shall be thereafter approved by resolution of the board of director or the corresponding body or function of each NIC.

The board of directors or the corresponding body or function of each NIC, in compliance with their own autonomy and independence:

(i) is responsible for the proper identification of any Area at Risk, General Standards of Control and/or Key Standards of Behaviour, in addition to those identified in Sections 9.1 and 9.2 of the GCG to be implemented through local internal procedures;

(ii) adopts the most appropriate measures for the implementation and monitoring of the GCG, taking into account the NIC's organization, complexity of business, specific risk profile and regulatory framework.

Each NIC will report changes or particular interpretations to the GCG which have been made in accordance with local legislation or customs.

Local Compliance Officer and Global Compliance Officer

The board of directors or corresponding body or function of each NIC shall identify the structure/structures (individual or body) in charge of: (i) providing support in the implementation and monitoring of the GCG; (ii) receiving the information flow regarding the implementation of the GCG through local internal procedures; and (iii) executing the related controls (the "**Local Compliance Officer**").

The Local Compliance Officer that has to be chosen within the local organization, in compliance with the following requirements:

1) **Required skills and competences**: the individual to be designated as Local Compliance Officer must have adequate skills and competences, that have to be determined by considering his/her background, his/her actual job

position, his/her ethical conduct and his/her previous training activity on ethical business standards;

2) **Empowering and Authority**: the NIC shall formally provide the Local Compliance Officer all necessary powers, authority and independence in order to perform his/her duties;

3) **Necessary means**: the NIC shall formally provide the Local Compliance Officer with all necessary means in order to perform his/her duties, i.e. all appropriate financial and human resources herein included.

The Local Compliance Officer has the following duties:

(i) Assure an adequate diffusion of the GCG within the NIC's organization;

(ii) Periodically inform Geox about all activities carried out to spread the knowledge of the GCG within the NIC's organization;

(iii) Monitor compliance operational processes to the GCG by carrying out appropriate audit activity;

(iv) Assure that all adequate disciplinary actions have been taken by appropriate internal functions in order to repress and punish any deviations from the ethical standards established by the GCG.

Furthermore, an internal function of Geox S.p.A. shall be appointed as "global compliance officer" (the "**Global Compliance Officer**") with the purpose to coordinate the activity of each Local Compliance Officer.

Such coordination activity will entail the Global Compliance Officer with the duty and the right to spread out guidelines and request tasks to each Local Compliance Officer in order to guarantee a proper and respectful observation of the contents of the GCG.

5. TRAINING AND COMMUNICATION TO RECIPIENTS

GEOX's Human Resources will arrange compulsory training sessions to be conducted periodically for all Corporate Recipients (including new employees) on the contents of this Global Compliance Guidelines.

Each NIC may evaluate – with the support of GEOX's Human Resources – to provide for specific training sessions for Corporate Recipients who are materially and directly involved in any Area at Risk.

GEOX's Human Resources is responsible for:

(i) planning and delivering the training sessions with the support of GEOX Internal Audit;

(ii) ensuring that each Corporate Recipient regularly attends training sessions; and

(iii) collecting attendance registration and copies of training materials and training dates.

The principles and contents of this GCG which are 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 GCG's Key Standards of Behaviour directly applicable to them.

6. REPORTING SYSTEM

When in doubt about the interpretation, implementation or compliance with any Area at Risk, General Standards of Control or Key Standard of Behaviour respectively, each Corporate Recipient shall consult with the LocalCompliance Officer before acting, using the e-mail address [•]

Furthermore, each Corporate Recipient shall report to the LocalCompliance Officer appointed by each NIC any suspected violation of this GCG or related policy, procedure or local instruction.

When contacted by the Local Compliance Officer or by the Global 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.

GEOX and each NIC will not tolerate 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.

Periodically, at least on a half-year basis, the Local Compliance Officer will inform the Global Compliance Officer about any misconduct or violation of the GCG.

Any report made to the Global Compliance Officer in accordance with this Section may be made by using the following e-mail: internalaudit@geox.com

Each NIC shall take any proper measure to grant confidentiality.

7. 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 NIC's function in the event of breach of any Key Standard of Behavior set out in the GCG, in accordance with the disciplinary system already in force, pursuant to applicable laws or local compliance programs and without prejudice for the protection afforded to employees under local legislation.

The disciplinary measures shall be applied despite the results of any possible criminal procedure carried out by the relevant judicial authority.

Each NIC will take appropriate measures, including but not limited to termination for cause of the relevant agreement, against Third Parties whose action are found to violate those Key Standards of Behaviour which are directly applicable to the latter.

8. CRIMES

The GCG applies to the following types of Crimes and illicit behaviours:

A. Bribery Crimes

B. Other Crimes against Public Entities

C. Accounting Fraud

D. Financing of Terrorism and Money Laundering Crimes

E. Market Abuse

F. Crimes against Individuals

G. Health and Safety Crimes

H. Environmental Crimes

I. Cyber and Privacy Crimes

J. Intellectual Property Counterfeiting Crimes and Consumer Fraud

Paragraph 9.2 below identifies the Areas at Risk to be monitored by each NIC and the applicable Key Standards of Behavior.

The list included in paragraph 9.2. does not prevent each Non-Italian Company from carrying out its own risk assessment and definition of additional Key Standards of Behaviour if deemed appropriate.

Therefore, each NIC might identify, if deemed appropriate:

(i) 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;

(ii) additional standards of behaviour which all Corporate Recipients and – where expressly specified – Other Recipients have to deal with in order to:

- abstain from any behaviour that gives rise to any of the Crimes described above; and
- abstain from any behaviour that, even though does not constitute itself any of the Crimes listed above, could potentially turn into.

9. THE GCG's CONTROL SYSTEM

The GCG provides for the following two main levels of control in relation to the Areas at Risk:

(i) General Standards of Control;

(ii) Key Standards of Behaviour applicable to each Area at Risk.

9.1 GENERAL STANDARDS OF CONTROL

In addition to the provisions set out in the Code of Ethics - which represents the Group's ethical principles to which all Recipients are required to comply - each NIC shall comply with the following General Standards of Control:

1. **segregation of duties**: the assignment of roles, tasks and responsibilities within a NIC shall be made in compliance with segregation of duties according to which no individual may autonomously perform an entire process (*i.e.* in accordance with this principle, no individual can be autonomously in charge of performing an action, authorizing it and subsequently check it); an adequate segregation of duties can be granted also using IT systems enabling only identified and authorized persons to perform certain transactions;
2. **power of signature and authorization**: formal rules shall be in place in relation to the exercise of internal powers and powers of signature. Powers of signature shall be consistent with the organizational and managerial responsibilities assigned to each proxy holder within the NIC;
3. **transparency and traceability of processes:** the identification and traceability of sources, information and controls carried out in relation to the formation and implementation of NIC's decisions, as well as the management of financial resources must always be guaranteed; proper storage of data and relevant information must be guaranteed, through information systems and /or paper support;
4. **proper management of Third Parties' relationships:**
    a) appropriate due diligence on honourability requirements shall be performed before any relationship is established. The extent of each due diligence assessment (which could include making enquiries through business contacts, local chambers of commerce, business associations, internet

searches or professional providers) 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;

b) additional checks and appropriate authorization levels, in the event that, during the due diligence phase, any "red flags" come up;

c) periodical monitoring during the course of the relationship to ensure that the counterparty continues to meet the requirements approved by the NIC, and

d) appropriate measures to be applied in the event that a Third Party does not maintain these requirements or any other “red flag” arise during the course of the contractual relationship.

9.2 AREAS AT RISK AND KEY STANDARDS OF BEHAVIOUR

A. Bribery Crimes and conflicts of interest

This type of Crimes is dealt with in the relevant Anti-Corruption Policy attached to these Global Compliance Guidelines as Annex 1.
Given the particular attention that GEOX reserves to contrasting this type of Crimes, both in the Italian territory and in the foreign countries in which the Group operates, not only Corporate Recipients shall make reference to Annex 1 for the relevant key standards of behaviour and all inherent duties, but also employees, directors and any other members of the management and control bodies of GEOX as well as consultants or other contractors and, in general, third parties who are respectively employed or appointed or who deal with or act on behalf of the GEOX shall make reference to Annex 1.

B. Other Crimes against Public Authorities

This type of Crimes mainly relates to fraud against public entities and occurs when a company executes an artifice or another illicit scheme in order to defraud a public entity to obtain any economic advantage.

Such type of Crimes is often connected to public funding and grants 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.

AREAS AT RISK

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

(i) participation to public tenders and public procedures in general;

(ii) management of relationships with public authorities (e.g. with reference to health, safety and environment requirements, management of personnel, payment of taxes);

(iii) application for public funding, grants, subsidies or guarantees issued by public authorities;

(iv) management of the received public funding, grants subsidies or guarantees obtained.

KEY STANDARDS OF BEHAVIOUR

In addition to key standards of behaviour set out in paragraph 9.2. lett. A. above, Corporate Recipients and Third Parties shall refrain from:

a) submitting false or altered documents, either fully or in part, during the participation to public calls for tenders;

b) carrying out cheating behaviours against a public authority which may induce the latter to make a wrongful assessment during the examination of requests for authorizations, licenses, clearances, concessions, etc.;

c) omitting due information in order to direct in the NIC's favor a public authorities' decisions in relation to any of the circumstances described at let. a) and b) above;

d) using sums received from public authorities as funds, contributions or loans for purposes other than those for which they were granted;

e) any conduct aimed at obtaining from a public authority any type of grant, funding, facilitated loan or other disbursements of the same type, by means of altered or falsified statements and/or documents, or the omission of necessary information or, more in general, by means of artifice or deception, aimed at leading the grantee institution into error.

Furthermore, in order to implement the behavioural standards described above, NICS are required to grant that:

a) 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;

b) 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;

c) the activities of collecting and analysing the information which are necessary for reporting purposes are carried out with the support of the competent functions;

d) 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.

C. Accounting Fraud

Accounting Fraud is a type of Crime mainly consisting in intentionally manipulating financial statements to create a false representation of a company's financial position towards investors, creditors, shareholders and other stakeholders.

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

- report false profits or losses;
- keep obtaining financing from a bank;
- tax evasion;
- 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 could be deemed to be at risk:

(i) drafting documents to be released to shareholders or to the public (e.g. financial statements, periodic financial reporting; etc.) regarding the assets and liabilities, revenues and expenses or cash flows of the NIC, even if such documents are other than the periodical accounting ones;

(ii) management of relationships with the external auditors (if any).

KEY STANDARDS OF BEHAVIOUR

The Non-Italian Companies are required to properly keep books, records and accounts, in a duly and accurate manner and in compliance with the applicable local laws.

Corporate Recipient and Third Parties, which have been assigned to keep books, records and account are required to properly act to ensure that:

a) data and information used for the preparation of periodic financial reporting are accurate and diligently verified;

b) all balance items, whose determination and quantification entail discretional valuations, are objective and supported by appropriate documentation;

c) invoices and other relevant documentation related to the transactions are properly vetted, recorded and stored;

d) 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;

e) access to such transactions records is allowed only in accordance with management's general or specific authorizations.

Furthermore, the Non-Italian Companies are prevented to perform any conduct which impedes and, in any case, obstructs the checking and auditing activities by any external auditors (if any) through the concealment of documentation or the use of other fraudulent means.

Finally, the Non-Italian Company are required to make all communications towards any public financial authority (as provided for by the local applicable law) in a correct, complete, proper and expeditious manner, not preventing them, in any way, from performing their duties, even in the context of any inspection.

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.

With regard to the money laundering, the following conduct, when committed intentionally, shall be generally regarded as money laundering:

(i) the conversion or transfer of property or money, knowing that such property or money is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or money or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

(ii) the concealment or disguise of the true nature, source, location or ownership of property or money, knowing that such property or money is derived from criminal activity or from an act of participation in such activity;

(iii) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity.

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 so as 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: support of terrorism.

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

- protection of the business, in countries where such terroristic organizations are rather influential;

- get more favourable economic conditions from a supplier;
- disguise the illegal origin of funds generated by the company.

AREAS AT RISK

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

(i) contractual relationships with clients, suppliers, consultants, partners and any other individual or corporation;

(ii) management of sponsorships and non-profit initiatives;

(iii) financial flows management.

KEY STANDARDS OF BEHAVIOUR

Each NIC shall prohibit 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, each NIC shall prohibit 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 each NIC is committed to implement all the requested preventive and subsequent control activities necessary to achieve that goal.

In particular, it is specifically forbidden to:

a) conclude any contractual agreement, sponsorship or non-profit initiative with a Third Party who has not successfully passed the due diligence process unless an authorization has been obtained through a proper escalation procedure;

b) make or receive payments on anonymous bank accounts or on bank accounts located in tax havens or "non-cooperative" countries;

c) issue or receive invoices or release documents in relation to non-existent transactions.

In order to implement the behavioural standards described above, each NIC must:

a) conduct proper due diligence on potential suppliers and partners or any other Third Parties, including candidate to sponsorship or non-profit initiative, using reliable, independent source documents, data or information. The due diligence activity shall be proportionate to the actual or perceived risk that these Third Parties can be involved in illicit activities. In this regard, the following circumstances can be considered red flags:

   (i) the Third Party is incorporated in a country that, according to international indices, such as the Transparency International Corruption Perceptions Index, is known for widespread corruption, or in a country which is considered as a "non-cooperative country" according to FATF blacklist or other international list prepared by international institutions in relation to the global fight against terrorism financing and money-laundering;

   (ii) the ownership structure of the Third Party appears unusual or excessively complex given the nature of its business;

   (iii) the Third Party has or had been suspended to join tenders or enter into contract with state-owned companies/public bodies/governmental agencies due to compliance investigations carried out by the public authorities;

   (iv) the Third Party has been already subject to criminal proceedings;

   (v) the Third Party refuses to comply with the compliance program adopted by the company and does not have in place any code of conduct or similar set of rules;

   (vi) the address of the Third Party's business is a virtual office;

   (vii) the Third Party has an undisclosed beneficial owner;

b) keep all records obtained through the due diligence measures (e.g. copies or records of official identification documents, inquiries to establish the ultimate beneficial owner, etc.);

c) respect local laws providing limits for cash payments;

d) adopt measures to perform analytical controls over the cash flows and management of bank accounts;

e) verify the validity of payments, by controlling that the beneficiary/payer, as the case maybe, is the actual counterparty involved in the transaction or contemplated within the contractual documentation.

E. Market Abuse

The Market Abuse offences generally might refer to three different patterns of conducts: (a) the purchase or sell of financial instruments, performed using a "price sensitive" information concerning such financial instruments which is not publicly available ("**Inside Information**") or the illegitimate communication of such information to third parties; (b) the alteration of the price-setting mechanism of financial instruments by spreading false or misleading information; (c) 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.

For example, Market Abuse Crimes could be committed in case a person:

- discloses Inside Information to a relative about an incoming acquisition inducing him/her to buy shares;
- spreads false information concerning the financial situation of a company in order to influence the price of its shares;

AREAS AT RISK

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

(i) 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;

(ii) management of Inside Information connected to listed companies and, particularly, listed companies of the Group and relevant financial instruments;

(iii) drafting of companies' prospectuses and financial statements;

(iv) any kind of transactions relating to financial instruments in portfolio.

KEY STANDARDS OF BEHAVIOUR

Each Recipient is expressly required to abstain from:

a) using Inside Information to carry out, either directly or indirectly, negotiation of financial instrument in order to obtain personal advantage or to favour Third Parties or a NIC;

b) recommending or inducing anybody, on the basis of Inside Information, to perform transactions on financial instruments;

c) disclosing Inside Information to Third Parties, except when this is required by law, or when such disclosure is requested by a public authority or is set out in specific contracts according to which the counter-parts are obliged to use the information just for the originally intended purpose and to maintain its confidentiality;

d) spread false or misleading information (whether about the NIC or about any other companies) through the media, the Internet, or else, in order to alter the market price of financial instruments;

e) perform any transactions on financial instruments against the applicable local market abuse regulations.

F. Crimes against Individuals

In a corporate framework the Crimes against Individuals are those offences referring to forced labor 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 child labour or exploitation of the workers.

Such Crimes could be committed should the NIC:

- exploit child labour;
- 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 workforce with minimal expenses;
- employ fully subservient workforce, to which no request would be refused.

AREAS AT RISK

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

(i) recruitment;

(ii) entering into contracts with Third Parties (contractors) (mainly those that utilize unskilled personnel);

(iii) entering into partnership with Third Parties (contractors) in countries where individual rights are not fully protected by legislation.

KEY STANDARDS OF BEHAVIOUR

Geox strongly condemns any form of forced labour or exploitation, whether it be in the form of child labour, or the exploitation of people with disabilities or pregnant women, or anyone who has not given their consent. The use of under-

age workers is only permitted in the context of applicable legislation being correctly applied and in compliance with the UN Convention on the Rights of the Child. More generally, the respect of human rights and of the rights of workers is of fundamental importance for Geox Group. That's why, as part of its work, it takes inspiration from the International Labour Standards (ILS) covered by the fundamental International Labour Organisation (ILO) conventions.

The NIC shall:

a) comply with any applicable local and international legislation (e.g. ILO conventions on the minimum age for employment and on the worst forms of child labor) on forced labor and workplace hygienic-sanitary conditions;

b) accurately verify the reliability of the Third Parties – in particular those which provide for non-technical services – in the selection process;

c) require the contractors to comply (and, in their turn, to require their subcontractors to comply) with any applicable local and international legislation (e.g. ILO conventions on the minimum age for employment and on the worst forms of child labor) on forced labor and workplace hygienic-sanitary conditions;

d) set forth in the agreements with such Third Parties specific and enforceable contractual penalties in case of breach by a contractor of any applicable international or local legislation addressing the issue in question.

G. Health and Safety Crimes

Health and safety crimes are mainly related to the compliance to local legislations and labor standards to be granted in the workplace to prevent employees' accidents and illnesses.

For instance, such Crimes could be committed in case a NIC, acting in infringement of the applicable health and safety legislation:

- omits to provide the necessary safety equipment to workers;
- omits to make first-aid available kit in the work-area;
- lets the employees work with in a dangerous environment;
- omits to have the employees periodically examined by a medical specialist in order to monitor their health and their psychic and or physical suitability for the activities they have to carry out;
- omits to provide protective gloves and masks to workers whose activities entail contact with dangerous materials.

These types of conducts can take place in the interest 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.

AREA AT RISK

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

(i) compliance with applicable health and safety laws.

KEY STANDARDS OF BEHAVIOUR

Regardless of the wideness of local legislation addressing health and safety in the workplace, NIC shall promote a strong culture of workplace safety protection,

increasing awareness regarding risks and responsibilities of individual behaviours.

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

In particular NIC shall:

a) consider the compliance to the provisions of law governing the health and safety of workers on the workplace as a priority;

b) 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;

c) correctly evaluate those risks which are not avoidable and adequately mitigate them by implementing appropriate individual and collective safety measures;

d) 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;

e) ensure that workers are periodically heard on matters regarding health and safety on the workplace;

f) 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;

g) timely consider and analyse any non-compliance or improvement area, emerged during the working activity or during inspections;

h) set the organization of the working activity in order to protect the integrity of workers, Third Parties and the community within which the NIC operates.

In order to keep properly monitoring the Areas at Risk, each Non-Italian Company assigns adequate 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

Environmental Crimes are related to a broad list of illicit activities, such as offences to wildlife, illicit trade and disposal of hazardous waste substances and many other acts which 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 examples, Environmental Crimes could take place if someone within a company:

- refraining from considering the local fauna when planning the activities to be performed and selecting the physical areas in which operate;
- refrains from properly performing Company's waste disposal and, on the contrary, sets up an illicit waste disposal site.

These types of conducts can be committed in the interest of a company for lots of reasons, such as:

- the reduction of costs, for by adopting the measures required to safeguard the environment a company is likely to incur in additional expenses;
- the increasing of productivity, as 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 could be deemed to be at risk:

(i) compliance with applicable environmental laws in connection with the activities carried out;

(ii) selection of the Third Parties which have to perform specific activities that can impact the environment (e.g. waste management and disposal).

KEY STANDARDS OF BEHAVIOUR

NIC shall consider the respect and protection of the environment as a priority and, in particular, it shall:

a) 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;

b) promote the use of energy from renewable sources and reduce waste;

c) adopt adequate waste disposal procedures in compliance with any applicable law (including any compulsory inscription to consortiums or associations) and with specific attention to dangerous waste;

d) reduce gas emissions in operations and comply with any applicable law;

e) 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;

f) adopt the appropriate instruments in order to prevent its activities to cause any form of damage and harm to the ecosystem.

I. Cyber and Privacy Crimes

Cyber Crimes are criminal offenses which relate to two separate categories of crimes: on the one hand, there are the misconducts whose target is a computer or a network, on the other hand, there are the crimes which are executed (or expedited) by means of a computer or similar devices.

The GCG addresses the former category of offences, which can consist, for example, in: (i) the unauthorized intrusion into a protected network; (ii) the introduction of computer viruses into a computer system; (iii) the interception of data from a computer network. For instance, Cyber Crimes could be committed by someone within a company in case 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.

Privacy Crimes are offences based on the violation of the right of individuals to respect for personal information ("personal data"). Privacy Crimes can be for example:

- processing of customers' data without their authorization in order to send them advertising (e.g. newsletters);
- unjustified remote control of workers;
- disclosure of customers or workers' images without their consent or appropriate release;
- customers' profiling for marketing purposes without their consent;
- fraudulent transfer of customers' data to third parties.

Several legislations (e.g. EU General Data Protection Regulation) protects persons' fundamental right to privacy, providing for specific rules with regard to the processing of personal data and asking companies to comply with such rules. In the light of the above, many behaviours, even if not criminally relevant, can nevertheless lead to the application of significant fines for companies.

Cyber Crimes and Privacy Crimes can take place for a number of reasons, such as:

- to access a competitor company's business secret or data;
- to obtain personal data (for example concerning customers' behaviours) or confidential information about competitor companies' market strategies;
- to jeopardize or damage a competitor company's computer system.

AREAS AT RISK

In relation to this category of Crimes, the following areas could be regarded as at risk:

(i) any company activity performed by using Intranet, Internet, the mail system or any other IT instruments;

(ii) management and protection of workstations, laptops, mobiles and storage devices;

(iii) planning of the measures to be adopted on telematics system as well as security, classification and processing of information and data;

(iv) processing of clients' personal data;

(v) processing of employees' personal data;

(vi) e-commerce management.

KEY STANDARDS OF BEHAVIOUR

Each Recipient shall refrain from incurring into (and NIC shall ensure, through the implementation of proper organizational, technical and physical measures) that the following misconducts are avoided:

a) the illicit access of Third Parties to the IT systems;
b) an improper use of IT credentials;
c) the 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;
d) the tampering or alteration of the NIC's computer system;
e) the exploitation of any lacks in the security measures of corporate IT system to gain access to the information without proper authorization;
f) the installation of software and databases without prior authorization;

g) the 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.);
h) the unlawful processing of personal data belonging to clients, employees or any other person.

NIC shall ensure compliance with any local applicable data protection law and 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.

The Non-Italian 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 and of the respect of any applicable data protection law.

J. Intellectual Property, Counterfeiting Crimes and Consumer Fraud

Intellectual Property Crimes and Counterfeiting Crimes refer to misconducts related to some infringements of copyright, trademarks and patents.

In particular, they generally relate to the use, without permission by the copyright holder, of works protected by copyright law, such as software, databases, videos, images, and music or to the manufacture, distribution or sale without permission of products which carry the trade mark or a patent belonging to a third party.

Consumer fraud takes many forms such as: false designation of origin of a product or false description of its characteristics with a view to deceiving the purchaser; publishing false advertisements or false prize (lottery or other contests for customers).

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 or the increase of sales by means of false advertisement.

AREA AT RISK

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

(i) company activities carried out using software and database;

(ii) marketing and sales activities;

(iii) use of images, video and music inside the stores;

(iv) production and distribution of products.

KEY STANDARDS OF BEHAVIOUR

Each Non-Italian Company shall adopt proper technical, physical and organizational measures in order to avoid:

a) any illegal use of trademarks and patents of third parties;

b) any counterfeiting of products;

c) any description and/or labelling of a product that does not fully correspond to the reality; (e.g. indicating a fabric composition that does

not fully correspond to the real one or indicating a product origin that does not fully correspond to the place of manufacturing, in breach of the applicable regulations);

d) any use of false or misleading information to advertise a product;

e) any illegal or deceptive practice concerning prizes or contests addressed to costumers;

f) any illegal use or dissemination, through computer based networks or through connection of any type, of protected original work, or part thereof;

g) any use, distribution, extraction, sale or lease of the contents of a database breaching the exclusive right of execution and authorisation from the copyright holder;

h) any use of images, video or audio contents breaching the exclusive right of execution and authorization from the copyright holder;

i) illegal download of any software without the execution of any proper contractual documentation;

j) the download of peer to peer software or any other software not directly connected to the corporate activity.

Should a NIC enter into a contract with external contractors for the performance of activities which could potentially be regarded as at risk of violating any copyrights rights, such contract must set forth provision by means of which the contractor commits to comply with applicable laws and regulation.