# ORGANISATION, MANAGEMENT AND CONTROL

## TAGETIK SOFTWARE S.r.l.

Pursuant to art. 6 Legislative decree. 231/01

**Reviews**

| Rev. | Review type | Board of Directors approval date |
|---|---|---|
| 0 | First version | 20.02.2012 |
| 1 | Overall review | 07.11.2017 |
| | | |
| | | |

## TABLE OF CONTENTS


| | | |
|---|---|---|
| 1. Definitions | 3 | Rev. 1 |
| 2. Introduction | 4 | |
| 3. Organisational and management Model | 6 | |
| 4. Supervisory Body | 10 | |
| 5. Internal information | 13 | |
| 6. Disciplinary system | 15 | |
| 7. Dissemination of the model | 18 | |
| SPECIAL SECTION "A" – Relations with Public Administration | Independent numbering Total pag. 3 | Rev. 1 |
| SPECIAL SECTIO"B" - Computer crimes and Offences involving the violation of copyright laws | Independent numbering Total pag. 3 | Rev. 1 |
| SPECIAL SECTION "C" - Corporate offences | Independent numbering Total pag. 4 | Rev. 1 |
| SPECIAL SECTION "D" – Market abuse | Independent numbering Total pag. 2 | Rev. 1 |
| SPECIAL SECTION "E" - Offences committed in breach of occupational health and safety regulations | Independent numbering Total. pag. 4 | Rev. 1 |
| SPECIAL SECTION "F" - Employ of citizens from third countries whose stay is irregular | Independent numbering Total pag. 1 | Rev. 0 |
| | | |

## 1. DEFINITIONS

| | |
|---|---|
| TAGETIK (or the Company) | Tagetik Software S.r.l. |
| Decree | Legislative Decree 8 June 2001 n. 231; |
| Addressee | Parties which are required to comply with the rules of conduct and the provisions set out in the Model: all those who work on behalf of TAGETIK SOFTWARE S.R.L., including administartors, auditors, corporate bodies, employes, collaborators (even temporary), trade partners, suppliers, supervisory body. |
| Entity or Entities | According to article 1 of the Decree, entities provided with legal status, companies and associations devoid of legal status to which the provisions of the Decree and the administrative liability apply; |
| Guidelines | Guidelines for the construction of the organisation, management and control Model pursuant to Legislative Decree 231/2001 published by Confindustria in its most recent version (March 2014); |
| Model | Organisation, management and control Model provided for by the Decree; |
| Predicate Offences | Offences for which the Decree has introduced the Entity's administrative liability. In particular, offences referred to in articles 24 and 25 et seq. of the Decree; |
| Consolidated Law | Legislative Decree 9 April 2008 n. 81. (so called Consolidated Law on the protection of health and safety in the workplac) and subsequent amendments and additions |
| TUF | Legislative Decree 24 February 1998 n. 58, Consolidated Law on Financial Intermediation and subsequent amendments and additions |

## 2. INTRODUCTION

### 2.1 The legal system of administrative liability of legal entities, companies and associations

The Legislative Decree no. 231 dated 8 June 2001 was issued in partial implementation of the Delegated Law no. 300 dated 29 September 2000 and regulates the concept of administrative liability of legal entities, companies and associations, including those without legal personality.
The Decree introduced into the Italian legislation the liability of entities for certain crimes (specified in art. 24 and ss. Of the Decree, so-called predicate offences) committed – or even just attempted, in the interests of or for the benefit of the Entities, or of an organizational unit with financial and functional autonomy, by:

(i) Persons holding representative, administrative or management role in the Entity or one of its organizational units (senior management pursuant to art. 5 of Decree, par. 1, lett. a); or

(ii) Persons under the management or supervision of one of the persons referred to in point (i) (subjects subordinate to the management pursuant to 5 Decree, first paragr. , lett. b).

The entity's liability is additional to that of the natural person who physically committed the offence and is intended to punish the Entities for the crimes committed for their benefit.
As a result of the liability introduced by the Decree, the Entity is subject to independent proceedings and is liable to penalties which may extent to stop the company's ordinary business.
Indeed, in addition to the financial penalties, the confiscation and the publication of the conviction sentence, the Decree establishes that the body can be also subject to restrictions of injunctive nature (art. 9, second paragr.), such as:

- Disqualification of company director;
- Suspension of revocation of license and permits used to commit the offence;
- Prohibition of entering into agreements with the public administration, other than obtaining a public service;
- The exclusion from concessions, loans, grants and subsidies and possible revocation of those already granted;
- Ban on advertising goods and services.

According to art. 4, Entities with head offices in Italy can be prosecuted also for crimes committed abroad if the legislation of the foreign Country does not provide for a similar form of criminal liability.
The entity's administrative liability is based on an "organizational liability": a Company is held liable for the offence together with the individual that committed it, where it has failed to create an organization structure that is effective in preventive such offences and, in particular, if it has omitted to set up an internal control system and establish suitable procedures in relation to the performance of activities in those area in which there is a greater risk of offences being committed.
On the contrary, as pursuant to art. 5 par. 2 od the Decree, the Entity is not responsible of the authors of the crime committed it in their own interest or in the interest pf third parties.
Art. 6 and 7 of the Decree describe how to set up an effective internal control and organization system:
- before the offence was committed, the managing body had adopted and effectively implemented appropriate organization and management models for preventing the offence in question;
- the task of monitoring the functioning and compliance of the models and their update was assigned to a corporate body with independent powers of initiative and control;

According to the Decree, with reference to the delegated powers and to the possibility that offences are committed, the model must fulfil the following requirements:
- identify activities in the context of which offences may be committed;
- envisage specific protocols for the planning and implementation of the entity's decisions regarding the prevention of offences;
- Identify appropriate methods of management of financial resources in order to prevent the commission of offences;
- establish disclosure obligations towards the body responsible for supervising the compliance and the functioning of the model;

- introduce a suitable disciplinary system envisaging penalties for lack of compliance with the rules indicated in the model.

The adoption of the Model, even though is not mandatory, has exceptional effectiveness of the administrative liability only if it is effectively implemented and constantly updated.

Indeed, the criminal proceedings judge has to assess, within the framework of the proceedings intended to ascertain the administrative liability of the Entity, the appropriateness of the Model to prevent crimes, as well as its actual application and effectiveness.

### 2.2 History, activities and governance of TAGETIK SOFTWARE S.R.L.

Tagetik Software S.r.l. has its operational headquarters in LUCCA, Via Roosevelt, 103 and its executive offices in Italy in Lucca (Via Borgo Giannotti, 37/U), Milan (Largo Richini Francesco, 6), Rome (Via Velletri, 24) and Turin (Corso Re Umberto, 3).

Tagetik was founded in 1986 as a Performance Management local consultancy.

Even though, at the beginning, it was just a small company on the Tuscan hills, rapidly became the fastest growing CPM solutions "software vendor".

During the 1990s, Tagetik expanded its business throughout Italy and developed its first suite of applications, composed of 4 products for the consolidation, the budgeting, the financial planning, the closing and allocation process.

In 1994 with Costa Crociere and then in 1997 with Ifil, TAGETIK SOFTWARE S.R.L. started to count among its clients some of the most important firms.

In 2002 UniCredit, the sixth biggest bank in the world chose Tagetik for the statutory consolidation. In this project, Tagetik collaborates with UniCredit and starts to develop Tagetik CPM.

In 2005 Tagetik launched Tagetik CPM (now Tagetik 5), the first completely unified product for the CPM processes and started to expand its business throughout other European countries.

In 2008 Tagetik opened two offices in North America. Shortly after, Gartner included it in the Visionary Quadrant of its "Magic Quadrant for CPM Suites".

Today, Tagetik is a global company and offers a unified CPM product on-premise and on the Cloud. With over 50.000 users in 40 different markets, counts among its clients some of the world's largest companies mentioned in Fortune 1000.

On the 6th of April 2017, Tagetik was acquired by Wolters Kluwer International Holding B.V. that therefore, as of today, is the sole shareholder of Tagetik Software S.r.l.

The management of Tagetik Software S.r.l. consists of a Board of Directors made up of 5 Members, some of which have specific powers (single signature) and others are Legal Representatives of the company.

From the operational point of view, the company counts 6 Departments that manage the organization and the development of the daily activities, within the scope of the general guidelines defined by the Board of Directors.

The organizational structure includes also some legal representatives, specifically for the Occupational Health and Safety, for the prevention of environmental crimes, the protection of data, the compliance with the privacy regulations and the financial/administrative management.

Dal 2012 Tagetik Software has been applying the Organization, Management and Control model described in this document and, as pursuant to art. 6 of Legislative Decree 231/01, has appointed the Supervisory Body responsible for monitoring the effective implementation of the Model.

The Organization, Management and Control model integrates with the company management systems and, in particular, TAGETIK SOFTWARE S.r.l. received from the International Body DEKRA CERTIFICATION S.r.l. the following certifications:

UNI EN ISO 9001 – Quality management system

BS OHSAS 18001 – Occupational Health and safety management system

UNI CEI ISO/IEC 27001 – Information Security Management System (applicable to Cloud services)

UNI EN ISO 22301 – Business Continuity Management

### 3.1 Purpose of the Organisational Model

The purpose of the Model is to establish a structured system of protocols and procedures, together with control and verification activities, with the aim of preventing, or at least reducing, the risk that the addressees of the Model may commit predicate offences.
Additionally, the purpose of the Model is to:

- Underline that such forms of illicit behaviour are strongly condemned by TAGETIK SOFTWARE S.R.L. as they are contrary not only to the law but also to the ethical principle to which TAGETIK SOFTWARE S.R.L. intends to adhere in the conduct of its business activities;
- Enable TAGETIK SOFTWARE S.R.L. to prevent and/or detect the commission of offences falling within the scope of the Decree, thanks to a system of controls, coupled with constant oversight of the proper implementation of the system, itself.

It follows that, in addition to the above, key elements of the Model are:

- the launching of staff training, awareness-building programmes focusing on the contents of this Model;
- mapping the TAGETIK SOFTWARE S.R.L. business areas in which the predicate offences might be committed;
- assignment to the Surveillance Board of TAGETIK SOFTWARE S.R.L. of specific surveillance tasks for effective and proper functioning of the Model;
- control and documentation of the activities at risk;
- compliance with the principle of segregation of duties;
- definition of levels of authority consistent with the responsibilities assigned;
- verification of the corporate behaviour ad of the Model functioning with consequent periodic update.

### 3.2 Structure of the Model

This Model is divided into a "General section" and several "Special sections", written according to the type of predicate offences TAGETIK SOFTWARE S.R.L. believes may be committed by the Addressees.
TAGETIK SOFTWARE S.R.L. understands that the implementation of the Model goes along with the adoption of an Ethical Code that formalizes the principles on which the company's business activities are based.
TAGETIK SOFTWARE S.R.L. does not mean to avoid this practice, especially since the Company's business activities have always been compliant with a set of principles and rules of conduct based on the values of honesty, transparency and good faith.
The original text of the Decree limited to identifying as predicate offences some crimes against the Public Administration and crimes against property (art. 24 and 25). Subsequent legislative reforms have expanded the number of predicate offences for which corporate liability applies:

- Computer crimes (art. 24-*bis*);
- Counterfeiting, legal tender and tax stamps (art. 25-*bis*);
- Crime against industry and trade (art. 25 *bis 1*);
- Corporate offences and bribery among private individuals (art. 25-*ter*);
- Crimes for the purpose of terrorism or subversion of the democratic order, as well as the practice of female genitals mutilation (art. 25-*quater*);
- Crimes against individuals (art. 25-*quinquies*);
- Crime of insider dealing and market manipulation (art. 25-*sexies*);
- Offences of manslaughter and negligence causing serious or very serious personal injury committed in concomitance with the breach of legislation of accident prevention and the protection of safety and hygiene at work (art. 25-*septies*);
- Crimes of money laundering, receiving of stolen goods and use of money, goods or benefits of unlawful origin and self-laundering (art. 25–*octies*);

- Offences involving the violation of copyright laws (art. 25 *novies*);
- Crimes against the judicial activity (art. 25 *decies*)
- Environmental crimes (art. 25 *undecies*)
- Employ of citizens of third Countries whose stay is irregular (art. 25 *duodecies*)

Further extension of the predicate offences will be provided for by the Decree in the near future.
For this reason, the Board of Directors of TAGETIK SOFTWARE S.R.L., also upon proposal of the Supervisory Body , will have to adopt specific deliberations to integrate the Module with new *Special sections* related to the offences that, as a result of further legislative interventions, will extend the scope of the corporate liability of the Company.

### 3.3 General Section

According to art. 6, paragraph 3, of the Decree (and according to the above mentioned Guidelines), the General section of the Model has three main purposes:

*I) Identify the Company's Activities within which Crimes could be potentially committed: mapping of risks*

Art. 6, paragraph 2, lett. a) of the Decree provides that the Model supplies the so-called mapping of risks:
First of all it is necessary to analyse the overall activity carried out by TAGETIK SOFTWARE S.R.L. and identify the operating or the decision making steps in which the Predicate offences may be committed.
Taking into account the legislative interventions that led to a gradual extension of the Predicate offences and given the changes that may occur in the corporate structure of TAGETIK SOFTWARE S.R.L. as well as in its activities, the mapping of risks can never be considered permanent and unchangeable but, on the contrary, must be constantly controlled, reviewed and updated.
TAGETIK SOFTWARE S.R.L., together with the Supervisory Body , will review and update, where necessary, the mapping of risks whenever new legislative interventions, changes in the corporate structure of TAGETIK SOFTWARE S.R.L. or just changes in the circumstances and/or in the procedures followed by TAGETIK SOFTWARE S.R.L occur.

*II) Definition of a preventive control system*

According to art. 6, paragraph 2 lett. b) of the Decree, after completing the mapping of risk, it is necessary to define specific protocols aimed at planning for the development and implementation of the entity's decisions regarding the identified at-risk areas.
For this purpose, specific measures (also with reference to internal procedures explicitly indicated) intended to prevent or at least mitigate the risk of crimes being committed, are described in each Special Section of this Model.
Besides these procedures having preventive purposes, the Supervisory Body can/has to perform later checks on single operations or on the corporate behaviour.
As with the mapping of risks, the adopted procedures can never be considered permanent: on the contrary, their effectiveness and completeness must be continuously verified by the Company and the Supervisory Body , which is also responsible for suggesting to the Board of Directors possible improvements, integrations and modifications.

*III) Designation of the Supervisory Body .*

The third purpose of the General Section is to appoint a Supervisory Body that, in compliance with the Decree, is tasked with:

- constantly verifying the compliance with the provisions of the Model and with the related procedures;
- constantly assessing the adequacy of the mapping of risks and of the procedures described in points I) and II);
- suggesting to the Board of Directors all the necessary amendments.

The Supervisory Body is a collective body of TAGETIK SOFTWARE S.R.L. but it is completely independent, as specified at point 4 of this document.

### 3.4 Special Sections

Besides the General section described before, this model includes some Special Sections, each related to a specific category of predicate offences TAGETIK SOFTWARE S.R.L. believes could be committed, according to the mapping of risks.

Each special section includes the description of the analysed crimes categories and specifies which business areas are considered at high risk and which procedures shall be adopted in order to avoid, or at least mitigate, the risk of those crimes being committed.
The Special Sections below analyse the following types of offence:
i) Crimes against the Public Administration (Special Section "A");
II) Computer crimes and Offences involving the violation of copyright laws (Special Section "B");
iii) Corporate offences and bribery among private individuals (Special Section "C");
iv) Market abuse (Special Section "D");
v) Offences of manslaughter and negligence causing serious or very serious personal injury committed in concomitance with the breach of legislation of accident prevention and the protection of safety and hygiene at work (Special Section "E");
vi) Crimes of money laundering, receiving of stolen goods and use of money, goods or benefits of unlawful origin and self-laundering (Special Section "F")
vii) Employ of citizens of third Countries whose stay is irregular (Special Section "G")
According to the mapping of risks carried out in 2012 and updated in 2017, TAGETIK SOFTWARE S.R.L. has decided to exclude from this Model the Crimes for the purpose of terrorism or subversion of the democratic order, as well as the organized crime, crimes against industry and trade and environmental crimes – for which anyway corporate liability applies – since real and concrete/significant risks of those crimes being committed does not exist, taking into account the specific business activities carried out by the Company.

### 3.5 Implementation of the Decree by TAGETIK SOFTWARE S.R.L.

In order to operate transparently and with integrity, as well as to protect the corporate reputation and the image of its partners, administrators and employees, TAGETIK SOFTWARE S.R.L. deemed it advisable to adopt and implement this Model and to keep it constantly up-to-date.
The Model has also the purpose to raise personnel's awareness of compliance with its principles in order to avoid and prevent crimes being committed while carrying out the business activities.
TAGETIK SOFTWARE S.R.L. prepared this Model with reference to its specific organisation, size and structure, the requirements of the Decree, the relevant court decisions, the Guidelines developed by the Trade Associations and those developed by Confindustria (version published on the website of Confindustria in March 2014).
The Board of Directors of Tagetik Software S.r.l has adopted this Model by special resolution.
Moreover, the Board of Directors appointed the Supervisory Body, currently composed of 2 members and endowed with autonomous powers of initiative and control and supervisory tasks in relation to the Model itself and in particular to its actual implementation, update and compliance with it.

### 3.6 Mapping of risks

Based on the provisions of the Decree and of the indications provided by the Guideline, TAGETIK SOFTWARE S.R.L. developed the mapping of risks, identifying the company's areas in which there is a greater risk of predicate offences being committed.
This section of the document briefly describes the methodology used for the development of the risks mapping.
First, TAGETIK SOFTWARE S.R.L. analysed the constituent elements of the predicate offences in order to identify types of conduct that, in the corporate context, could constitute offences.
Then, TAGETIK SOFTWARE S.R.L. analysed the corporate context, in order to identify the areas and the sectors at greater risks. The analysis of the areas at risk was conducted with the support of a lawyer and of an external consultant expert in corporate organisation; the analysis of the TAGETIK SOFTWARE S.R.L. Company was based on interviews with the Administrators and the Process Managers and on the analysis of sample documents used for the management of the company's activity. The mapping of risks was updated in 2016 with the support of the Supervisory Body.
Finally, TAGETIK SOFTWARE S.R.L. developed specific procedures and protocols aimed at ensuring compliance of the model is compliant with the provisions of the Decree. The results of the risks mapping process will be

thoroughly described in the Special Sections together with the measure and procedures implemented by TAGETIK SOFTWARE S.R.L. in order to avoid, or at least mitigate the risk of predicate offences being committed.

### 3.7 Addressees

The principles and contents of the Model are addressed to all those who work on behalf of TAGETIK SOFTWARE S.R.L., including administrators, members of corporate bodies, employees, collaborators (even temporary) i collaboratori anche occasionali, business partners and members of the Supervisory Body.

## 4. Supervisory Body

### 4.1 Appointment of the Supervisory Body

The Supervisory Body of TAGETIK SOFTWARE S.R.L. in an internal body endowed with autonomous powers of initiative, control, and supervisory tasks in relation to the Model itself and in particular to its actual implementation, update and compliance with it.
The Supervisory Body of TAGETIK SOFTWARE S.R.L. is composed of two members with proven expertise and experience that will adopt a special regulation for its proper functioning.
TAGETIK SOFTWARE S.R.L. appointed as members of its Supervisory Body two professional experts in the contents of the Decree: a statutory auditor and chartered accountant, previously appointed as Chairman of the Board of Auditors of Tagetik Software Srl, and an expert in Corporate Organisation who has known the company for years.
This is considered by TAGETIK SOFTWARE S.R.L. to be an ideal solution since it allows the Supervisory Body to work effectively, because it is composed of external members that have a thorough knowledge of the corporate structure of TAGETIK SOFTWARE S.R.L. and of how the company carries out its business activity.
The Supervisory Body is elected by the Board of Director of TAGETIK SOFTWARE S.R.L. for the period specified at the time of its appointment or, if not specified, for a period of three years. Its members can hold this role for an undefined number of mandates.
The following circumstances are cause for ineligibility and/or loss of office of the members of the Supervisory Body:
i) having been convicted, even if with non-definitive or plea-bargaining sentence, for crimes punishable as general malice, therefore excluding the accidental crimes, except those referred to in article 589 and 590 par. 3 p.c., committed in violation of the regulations concerning safety and hygiene and health protection at work, as well as offences that entail the application of accessory penalties prescribed by article 19 p.c., or required by specific law provisions;
ii) any conviction, even with non-definitive sentence, that entails the application of accessory penalties prescribed by art. 19 p.c. or required by specific law provisions;
iii) the application of patrimonial or personal security measures, the application of personal or patrimonial prevention, or the application of measures of anti-mafia prevention;
iv) statement of interdiction or inability pursuant to the Italian Civil Code, as well as conflict of interest with TAGETIK SOFTWARE S.R.L..
Moreover, another cause for loss of office is the application of a remand order (preventive detention, home detention, obligation to stay at a designated place, order of daily attendance at the judicial police office, travel prohibition) and the application of a prohibitive measure (suspension from public service activity, temporary suspension from professional activity).
The Italian Civil Code regulations will apply to the Surveillance Body and its members.

### 4.2 Main characteristics and resources of the Supervisory Body

The Supervisory Body can avail itself of the collaboration with people from various business activities, where their expertise becomes necessary for specific analysis and for the assessment of specific operating and decision-making steps of TAGETIK SOFTWARE S.R.L. business activity.
At any rate, the Supervisory Body can benefit from the consultation of external experts, when necessary.
The Supervisory Body, at the start of its mandate, and then on an annual basis, can submit to the Board of Directors of TAGETIK SOFTWARE S.R.L. an annual budget request. In particular:
• the Supervisory Body will submit to the Board of Directors the request for the amount reported in the annual budget with details of costs and expenses for the correct related to the proper fulfilment of the mandate;
• the Board of Directors reasonably cannot refuse to provide such amount, without prejudice to the fact that the Supervisory Body can use it, autonomously and with no obligation or prior authorization, for the purposes foreseen in this Model;

• this amount must cover the expenses that, according to the estimates, the Supervisory Body will incur to carry out its functions (without prejudice to the fact that any costs relative to the human resources or to the equipment provided by TAGETIK SOFTWARE S.R.L. are not included in the budget);
If, because of exceptional events or circumstances, the Supervisory Body needs a supplemental amount in addition to that specified in the budget, the Chairman of the Supervisory Body will have to address a reasoned request to the Board of Directors of TAGETIK SOFTWARE S.R.L. specifying in detail the reasons for such request. The Board of Directors cannot reject the request for additional funds without just cause.

### 4.3 Duties and Powers of the Supervisory Body

The Supervisory Body of TAGETIK SOFTWARE S.R.L. is tasked with:
- supervising the functioning and the compliance of the model;
- supervise the functioning of the Model with regard to prevention of commission of the offences;
- providing for its update and submitting the relevant proposals to the Board of Directors;
- notifying the Board of Directors of verified infringements of the Model so that it can take the necessary measures.

Without prejudice to the obligation of the Supervisory Body to supervise the compliance with the Model and its regulations, the Board of Directors cannot criticise its work, unless in case of noncompliance with its mandate.
In particular, in order to fulfil these purposes the Supervisory Body of TAGETIK SOFTWARE S.R.L. will:
- carry out inspections on regular basis on the business activities in order verify compliance with the Model and to update the mapping of the at-risk areas;
- ask for specific information on a regular basis to each department in relation to the activities that are considered to be at risk. The information requested by the Supervisory Body must be provided by the involved departments with no omission nor modification in order to provide the Body with a concrete vision of the activities under inspection; for this purpose, the Supervisory Body must be constantly notified of the development of the areas at risk and has free access to the company documentation.
- work along with the other departments (also through specific meetings) to improve the monitoring of the activities in the areas that are considered to be at risk;
- coordinate with the heads of the company departments to guarantee compliance with the Model;
- verify that the required documentation is up to date and compliant with the content of each Special Section of this model;
- control, on a regular basis and in a target-oriented manner, the actual performance of procedures operations or activities within TAGETIK SOFTWARE S.R.L. ;

Moreover, the Supervisory Body will:
- verify the adequacy of the existing rules in relation to changes in the company activity;
- notify the Board of Directors of flaws in the Model and of any suggestion for improvement or modification;
- provide for the update of the rules of conduct of each Special Section;
- verify the validity of the standard clauses aimed at the implementation of penalty mechanisms (e.g. those concerning the termination of contracts with trade partners, collaborators or suppliers) in case of breach of the provisions set out in the Decree;

The Supervisory Body will have to submit an information report to the Board of Directors, on an annual basis.
Finally, according to art. 6, par. 1 lett. b) of the Decree, the Model update and monitoring activities can be divided as follows:

- *checks on proceedings:* the Supervisory Body will check, on a regular basis, the main proceedings and any relevant contract concluded by TAGETIK SOFTWARE S.R.L. within the areas at risk;
- *Checks on procedures:* the Supervisory Body will verify, on a regular basis, that the Model is actually being implemented;
- *checks on reports and measures:* the Supervisory Body will analyse each report received during the year, the actions taken in this regard and the most dangerous events; it will also verify that all Addressees of the Model know its content and are aware of the offences for which corporate liability applies.

The results of such verification will be included in the annual report the Supervisory Body provides to the Board of Directors, to the Board of Auditors and to the Shareholders' Meeting.

## 5. INTERNAL INFORMATION FLOWS

### 5.1 Communications and reports to the Supervisory Body

The Supervisory Body of TAGETIK SOFTWARE S.R.L. can be contacted in 3 different ways:

- Personal contact with one of its members and execution of a document addressed to the Supervisory Body
- @-mail to organismodivigilanza@tagetik.com
- Written reports, even into anonymous form, in a closed envelop to the address: Organismo di Vigilanza c/o Tagetik Software S.r.l., Via Roosevelt, 103 55100 LUCCA.

The supervisory body shall carry out internal investigations after receiving reports of violation of this Model and, if such reports are valid, it shall give non-binding opinions on the type of actions to take and on the possible sanctions against the culprits. The Board of Directors is responsible for applying such measures and sanctions. The Supervisory Body shall protect those making reports from retaliation, unlawful conditioning or penalization.

### 5.2 Information obligations to the Supervisory Body

Besides the documentation explicitly provided in each Special Section of this Model, it will be necessary to notify the Supervisory Body of any information relating to the implementation of the Model in the at-risk areas, as well as of breaches of the requirements set out in the Model itself.
The following information must be provided to the Supervisory Body:
- decisions related to the request, supply and use of public financing;
- requests for legal assistance presented by employees (including managers);
- measures and/or information from the Judiciary and from the Police bodies or any other authority, proving that investigations are being carried out, even against an unknown person, for facts involving the business activities of TAGETIK SOFTWARE S.R.L.;
- results of committees of inquiry or other internal reports which reveals hypothesis of liability for the Predicate Offences;
- information about the implementation of the Model;
- disciplinary measures, sanctions imposed, or act of dismissal of these proceedings with the related reasons;
- tenders summary tables of public tenders or private negotiations;
- procurement contracts awarded by public entities, by the EEC or persons who perform functions of public utility;
- serious or very serious workplace injuries and accidents (approximately with a prognosis of more than 40 dd)

The Board of Directors must inform the Supervisory Body of any issue that falls within the competence of the Supervisory Body itself.
In order to enable the Supervisory Body to efficiently carry out the task it has been assigned, TAGETIK SOFTWARE S.R.L. allows all Addressees of this Model to notify this body of any offence, anomaly or suspicious activity, in relation to the commission of predicate offences.
TAGETIK SOFTWARE S.R.L. will protect all those who will notify the Supervisory Body from any form of retaliation, discrimination or penalisation, and guarantees confidentiality about the reporter's identity.
All employees of the company have the authority – and the duty – to communicate in written any information related to possible internal anomalies or unlawful activities.
The Supervisory Body can receive and assess written communications from persons from outside of the company.
The Supervisory Body can ask the Board of Directors or the employees for any type of information and/or documentation, for the purposes of control.
The Supervisory Body of TAGETIK SOFTWARE S.R.L. shall receive from the Board of Directors detailed information about any modification to the tasks and delegations assigned.
The Supervisory Body verifies and analyses the received information and the communications, and the actions to take; the measures must comply with the provisions set out in the Model.
The Supervisory Body can ask the Board of Directors for the application of disciplinary measures against those who fail to meet the information obligations.

The Supervisory Body will inform the Board of Directors if, according to the verification on the received information and communications, these were written with malicious intent or serious misconduct with the purpose to hurt the company, its managers and employees.

### 5.3 Information obligations of the Supervisory Body towards the corporate bodies

The Supervisory Body must meet information obligations towards the Board of Directors and the Shareholders' Meeting.
Moreover, the Supervisory Body must provide prompt information on any change, integration or update involving the Decree. The Supervisory Body must also notify the Board of Directors of any infringement verified when carrying out their activity.
At any time, the Board of Directors can call the Supervisory Body of TAGETIK SOFTWARE S.R.L. who, in turn, can ask to talk to the Board about the implementation of the Model or specific circumstances.
Moreover, the Supervisory Body annually provides the Board of directors (and the Shareholders' Meeting) with a written report of the Model.

### 5.4 Collection and storage of information

The Supervisory Body will store the received information and reports into a specific computer or paper archive accessible to third parties under specific procedures defined by the Supervisory Body itself.
Obviously, this documentation will be available to the Supervisory Bod and anyone who is interested in examining it.
The Supervisory Body has decided to use a minutes book with stamped pages.

## 6. DISCIPLINARY SYSTEM

### 6.1 General principles

According to Article 6 paragraph 2 e) of the Legislative Decree, a disciplinary system must be introduced in order to effectively penalise the infringements detected.
The disciplinary system (to be adapted to the type of offence) to apply in case of breach of the Model's provisions, makes the surveillance and prevention activities effective and aims to guarantee the effectiveness of the Model itself.
The disciplinary system is based on the following principles:
• differentiation according to the Addressees of the Model;
• definition of the disciplinary measures to apply against the addressees in compliance with the provisions set out in the collective agreement and the applicable legislative requirements;
• definition of procedures aimed to ascertain breaches, infringements, faulty or incomplete application, as well as a procedures of imposing penalties along with the appointment of the person in charge of monitoring the compliance with, the application and the update of the disciplinary system.
In particular, the disciplinary system is addressed to:
- all those who perform representative, administrative and executive functions (including any liquidations officers) at TAGETIK SOFTWARE S.R.L.;
- those subject to the direction or supervision of the former and, more in general, all employees of TAGETIK SOFTWARE S.R.L. that contribute to the overall business activity, as well as associates, trade partners and vendors.
This disciplinary system is composed of specific sections, each addressed to a specific category of addressees, according to the legal status of the various parties concerned.
The supervisory body is responsible for monitoring the compliance with the disciplinary system and for taking the appropriate actions to enable the Board of Directors of TAGETIK SOFTWARE S.R.L. to update, modify and/or complete the disciplinary system itself.
The application of disciplinary penalties disregards the result of possible criminal proceedings, since the rules of conduct imposed by the Model are adopted by the company in complete autonomy, independently of any unlawful behaviour.
The Supervisory Body can propose to the Board of Directors of TAGETIK SOFTWARE S.R.L. the adoption of disciplinary measures based on the seriousness of the ascertained infringements.

### 6.2 Sanctions applicable to employees

Any conduct by the employees in violation of the rules of conduct set out in the Model will constitute disciplinary offences.
The sanctions applicable to the employees are those defined in the national labour collective agreement, in accordance with the procedures referred to in article 7 of the law 30 May 1970, n. 300 (so called Statute of labourers) and any existing special regulations.
In particular, the sanctions imposed according to the seriousness of the violation, can be those provided for in Collective Agreement, and in the national labour contract for Marketing Managers.
Sanctions will be imposed, in accordance with the procedures established by the applicable Collective Agreement, by the Board of Directors, on its own initiative or upon the proposal of the Supervisory Body. .
As for the occupational health and safety, the application of disciplinary sanctions can be asked by the prevention and protection service Manager and/or by the employer.
The disciplinary measures described below are those provided for in Collective Agreement and take into account:

- the Intentionality of the behaviour and the degree of negligence, imprudence or unskilfulness with regard to the foreseeability of the event;
- the overall conduct of the employee, with particular regard to the existence or lack of previous disciplinary measures against the employee, within the limits permitted by law;

- the role of the employee;
- the functional position of the personnel involved in the facts constituting the violation;
- other specific circumstances surrounding the disciplinary infringement.

No changes occur to the provisions of art. 7 law 300/1970 and these provisions are here referred to in relation to the posting-up of the disciplinary codes, and in particular to the obligation to notify previously the charge to the employee, also in order to allow the employee to prepare an adequate defence and to provide any justification.

Therefore, the disciplinary actions that may be taken against the employees, in compliance with the provisions of art. 7 of the Statute of Labourers (L. 20 may 1970, n. 300) and any existing special regulations, are those defined in the collective agreement:

1. Verbal reprimand: minor non-compliance with the internal procedures set forth in the Model or negligent conduct that is not compliant with provisions of the Model.
2. Written reprimand: recidivism of offences at point 1.
3. Fine not exceeding the amount of 4 hours of the normal remuneration: noncompliance with the principles and rules of conduct described in the Organisational Model and/or in the Code of Ethics, namely in the event of breach of the internal procedures and rules, to the extent to be considered even if not minor, however not serious, since the said conduct is connected to a minor non-compliance with the contractual rules or directives and instructions issued by the management or superior.
4. Suspension form work without pay for 10 days: noncompliance with the principles and rules of conduct described in the Organisational Model and/or in the Code of Ethics, namely in the event of breach of the internal procedures and rules, to the extent to be considered relatively serious, or it is recurrent in any disciplinary offence sanctioned with a fine.
5. Disciplinary dismissal without notice: applies in case of serious and/or repeated violations of the rules and/or procedures and/or internal regulations established by the Organisational Model and/or by the Code of Ethics, although it is only likely to configure any of the offences penalised by the Decree.

In case of noncompliance – by the executives - with the rules and principles of the Model and of the Code of Ethics, namely in case of failure to comply with the internal regulations, in case of adoption, within the Sensitive Activities, of non-compliant conduct or a conduct not adapted to the aforesaid provisions, those responsible will be subjected to the most suitable measures foreseen by the National Collective Employment Contract for Industrial Executives. Executives failing to supervise the correct implementation of the rules and procedures envisaged by the Model and the Code of Ethics by subordinate workers, as well as breaching the rules of conduct set out in the model, also commit a disciplinary offence.

This disciplinary system is constantly monitored by the Supervisory Body and by the Board of Directors. The Organisational Model and the Code of Ethics are considered to bind all addressees. Therefore, the company discloses these documents and their later updates to the addressees by an internal newsletter in compliance with art. 7 of the Statute of Labourers, focusing on the specific penalties for the offences.

### 6.3 Sanctions applicable to Directors and Statutory Auditors

If the directors of TAGETIK SOFTWARE S.R.L. fail to comply with the rule and principles of the Model, the Supervisory Body will inform the Board of Directors and, if considered appropriate, the Shareholders' Meeting who will take the appropriate actions according to the applicable regulations.

### 6.4 Sanctions applicable to collaborators, trade partners and suppliers

Any conduct adopted by collaborators, trade partners and suppliers that is not compliant with the code of conduct set out in the Model and might entail the risk of committing predicate offences causes, in accordance with the contractual terms included in the letters of appointment or in the *partnership* agreements, the termination of the contract, without prejudice to the request for compensation for damages to TAGETIK SOFTWARE S.R.L., e.g. where the Judicial Authority applies the sanctions set out in the Decree

## 7. DISSEMINATION OF THE MODEL

The basic prerequisite for the Model exempting the Company from the corporate liability is its effectiveness along with its actual application.
The compliance with the Model can be achieved only through the dissemination of the Model itself to all addressees.
Therefore, TAGETIK SOFTWARE S.R.L. has taken the initiatives described here below in order to guarantee the correct knowledge and disclosure of the Model not only within the company but also outside of it.

### 7.1 Staff training

TAGETIK SOFTWARE S.R.L. promotes the knowledge of the Model among all the Addressees who are required to know and comply with its content as well as to contribute to its effective implementation.
The staff training (including the external consultants) will be structured are follows:

- Initial training through specific meetings immediately after the approval of the Model and its future revision.
- Disclosure of an internal summary note about the Model and its purpose;
- Publication of the Model and of the Code of Ethics on the website and on the intranet of TAGETIK SOFTWARE S.R.L.;
- Publication of the internal procedures related to the Mode on the intranet of TAGETIK SOFTWARE S.R.L.;
- Dissemination, through internal newsletter, of relevant informational material and constant and prompt communication of any updates or modifications;
- Information provided upon hiring.

### 7.2 Dissemination of information to collaborators, trade partners and suppliers

TAGETIK SOFTWARE S.R.L. promotes the knowledge and compliance with the Model among collaborators, trade partners and suppliers, through the publication of this Model on the company's website.

### 7.3 Contract Terms

In order to guarantee compliance with the provisions of the Model by third parties that contribute, even indirectly, to the business activities of TAGETIK SOFTWARE S.R.L., the Company will include in the appointment contracts and letters agreed with trade partners, suppliers and collaborators, specific contract clauses through which the subscribers agree to comply with the regulations of the Model and accept that failing to comply with them can cause the termination of the contract by TAGETIK SOFTWARE S.R.L..
The company believes that this contractual remedy is the only instrument that helps to guarantee compliance with the principles and procedures set out in the Model by third parties (such as collaborators, trade partners and suppliers) who are not subjected to the sanctions applicable to the employees.

## SPECIAL SECTION "A"

### Relations with Public Administration

**1. Type of offences in dealings with Public Administration (articles 24 and 25 of Decree)**

This Special Section shortly describes the specific offences referred to in articles 24 and 25 of the Decree:

*Embezzlement against the State or the European Union (art. 316-bis p.c.)*

This offence occurs when, after having received financing or contributions from the Italian State or the European Union, such funds are not utilised for the purposes for which they were intended (the conduct, as such, consists in having diverted, even partially, the funds received, without being able to demonstrate that the planned activity has nevertheless been completed). Taking into account that the time of perpetration of the offence coincides with the executive phase, the said offence may comprise also financing already obtained in the past but not subsequently utilised for the purposes for which it was granted.

*Misappropriation of funds to the detriment of the State or of the European Union (art. 316-ter p.c.)*

This Offence occurs when – on hand of the utilisation or the presentation of false declarations or documents or the omission to provide required information– financing, preferential interest rate loans or other similar contributions are unjustifiably obtained from the Italian State, from public utilities or from the European Community.

In this case, contrary to the preceding point (Article 316-bis), the purpose for which the funds are utilised is irrelevant, in bis), the purpose for which the funds are utilised is irrelevant, since Offence is committed at the time when the funds are received

Finally, it should be noted that such Offence is of a reductive nature in regard to fraud to the detriment of the State, in that it applies only [...] in those cases where the conduct does not provide sufficient grounds for a charge of fraud to the detriment of the State.

*Concussion (art. 317 p.c.)*

This Offence is committed when a government official or person responsible for a public service, abusing his role, compels another party to provide him or other persons with money or other benefits to which they are not entitled.

This Offence is subject to a merely reductive application within the context of the offences contemplated by Legislative Decree; in particular, it may be possible to recognise the relative grounds for prosecution within the application of Legislative Decree itself, when an employee or agent of the company concurs to the commission of the Offence by the government official who, taking advantage of such capacity, requests services from third parties to which he is not entitled (provided that, as a consequence of such conduct, the company in some manner derives a benefit).

*Corruption for an official function or action contrary to official duties (art. 318-319 p.c.)*

This Offence is committed when a government official accepts, for himself or on behalf of other parties, money or other benefits to perform, omit or delay the performance of official acts (thus determining a benefit for the party offering the bribe).

The activity of the government official may be influenced, be it to perform an official act (e.g. to give priority to matters which are part of his normal duties), be it to act in contrast with his duties (e.g. acceptance by a government official to ensure a tender award).

This type of offence differs from concussion, in that there is an agreement between the corrupting and corrupted parties intended to attain a mutual benefit, whereas in the case of concussion the conduct of the government official or the person responsible for the public service is imposed upon the private party.

*Instigation of bribery (art. 322 p.c.)*

This Offence arises when, faced with a conduct aimed at bribery, the government official refuses the illicit offer made to him.

*Bribery in judicial acts (art. 319-ter)*

This offence is committed when the company is involved in legal proceedings and, in order to obtain an advantage in the legal proceeding itself, bribes a government official (not only a magistrate, but also clerk of the court or other officer).

*Fraud against the State or other Public Body or the European Union (art. 640, par. 2, n. 1, p.c.)*
This offence is committed when an unfair profit is achieved, to the detriment of the State (or other Public Body or to eh European Union).
This offence could involve, for example, providing a public body or such like with incorrect information contained in the documents or data necessary for participating in tenders in order to win the tender in question.
*Aggravated fraud for the obtainment of public grants (art. 640-bis p.c.)*
This Offence arises when the fraud is committed in order to illegally obtain Government Grants.
These events may occur if subterfuge or deception are used, for example by communicating untruthful data or by preparing false documentation to obtain public funds.
*Computer fraud against the State or other Public Body (art. 640-ter p.c.)*
This offence occurs when someone, by altering the operation of a computer or telematic system, or manipulating the data contained therein, obtains an unfair profit to the detriment of third parties.
As a practical example, once the grants have been received, this Offence could be committed through the unauthorised access to the information system in order to attribute a higher value to the financing than the funds legitimately received.

## 2. Assessment of areas at risk

Regardless of the fact that the risk of crimes being committed against the Public Administration involves any business activity (all companies, in carrying out their business activities, often deal with different public bodies and for different reasons, firstly the formation of the company, with reference to the registration and disclosure requirements), the risk of offences against the Public Administration is considered irrelevant for TAGETIK SOFTWARE S.R.L. Even though its clientele basically consists of private companies, in some cases the recipients of the services of TAGETIK SOFTWARE S.R.L. are public companies or companies in which public authorities have a majority holding (municipally owned companies), following this assessment, ethical principles in the management of the relations with public administration have been inserted in the corporate Code of Ethics and specific procedure have been introduced in order to reduce and control the risk of offence.

## 3. Identification of the activities at risk

The prerequisite for such offences is the relation with the Public Administration (understood in the broad sense and including also the Public Administration of Foreign Countries, as well as representatives of private bodies that carry out activities which are governed by public law).
All business activities that imply relations with the Public Administrations shall be considered at risk (activities of direct risk).
Those business activities that do not imply any relation with the Public Administration but entail the use of financial and payment instruments, as well as other activities that may bring any benefits to public officials (or related subjects) through the perpetration of crimes against the Public Administration (activity of indirect risk) shall be considered at risk as well.
The followings constitute areas of indirect risk (with reference to the likelihood that these could be used to create hidden reserves of money for illegal payments or for concealing such illegal payments):
• administration, financial, accounting and fiscal activities;
• payment activities, with reference to the hypothesis that the selected subjects might be connected to public officials and local administrators and, therefore, the assignment might be part of a corruptive process or other unlawful benefit;
• the award of professional consultant agreements, especially when the selected subject works in close contact with the public administration area TAGETIK SOFTWARE S.R.L. is dealing with;
• recruitment;
• appointment of senior managers and members of corporate bodies.

## 4. Principles of conduct in the management of activities exposed to direct risk

This special section expressly forbids the Addressees from:
I) adopting behaviours liable to constitute the above offences (art. 24 and 25 of the Decree);

II) adopting behaviour that, although per se do not constitute offences included in the above, may potentially become such or be subject to misinterpretation;
III) giving rise to any conflict of interest vis-à-vis the Public Administration with regard to the matters covered by the aforementioned offences.
With regard to the relations with the Public Administration, it is forbidden to:
a) give cash gifts to public officials;
b) No gifts which may influence independence of judgment or induce the grant of any advantage to the company may be made to Italian or foreign public officials (even in countries in which such gifts are common practice) or to members of their families. Only gifts of little value, such as gadgets and products expressly approved by TAGETIK SOFTWARE S.R.L. are exceptionally allowed.
c) grant any type of benefit (job offers, etc.) to public officials of the Public Administration that might lead to the consequences set out in point b);
d) carry out services in favour of commercial partners that maintain business relations with the Public Administration, which do not find sufficient justification in the context of the contractual relation constituted with them;
e) make payments to collaborators that work with the public administration and which are not adequately justified in relation to the type of work to be carried out;
f) submit untrue or incomplete declarations to national or European Union public bodies in order to win public tenders or obtain contracts from public companies and/or companies in which the public authorities have a majority holding, award public grants, contributions or subsidised loan, or any other result;
g) allocate sums received from national or European Union public bodies, in the form of grants, contributions [...] or loans for purposes other than those to which they were assigned.
Any relation with the Public Administration must follow the basic principles set out in the company's Code of Ethics, as well as the following precepts:
- *formality*: it is appropriate to follow formal procedures and avoid – as far as possible - informal relationships with public administrators;
- *traceability*: it is necessary to leave written traces of the main phases and of the contracts during the administrative proceedings.
- *control:* participation in tenders, award of contracts and supply of services towards the public administration must be verified by the appointed functions and, if necessary, by the Supervisory Body.

**5. Principles of conduct in the management of activities exposed to indirect risk**

As stated before, the Model shall include further checks on some activities that could provide the opportunity to use sums of money for corrupt purposes or to confer benefits and appointments that might hide unlawful donation. In particular:

- Participation in tenders and/or stipulation of contracts with companies in which the public authorities have a majority holding

Participation in tenders and/or stipulation of contracts with public companies and/or companies in which the public authorities have a majority holding must be carried out with a scrupulous attention to transparency, compliance with the rules of fairness and truthfulness of the declarations made

- Payments management

This activity follows the relevant internal procedure that implies the intervention and/or the authorization of at least two persons. The payment of all invoices, except small value invoices, must follow the established procedure.

- Recruitment

The personnel selection is supervised by Head of Human Resources, in accordance with the relevant internal procedure.

- Appointments to external professionals and consultants

Engagements are assigned to external collaborators, consultants and professionals through engagement letter and/or written contract, providing details about subject and fee. The involvement of external consultant or

professionals goes along with the supplier verification as provided in the procedure for Services towards Public Administration.

**6. Internal reference procedures and documents**

With regard to this special section, the following internal documents and procedures are available:

1- Code of Ethics
2- IT Purchase Procedure
3- Marketing Purchase Procedure
4- Goods and Services Purchase Procedure
5- Business Agents Management Procedure
6- Trade Procedure
7- Expense Reimbursement Procedure
8- HR Procedure
9- Procedure for tenders and provision of service to the Public Administration

These procedures complete the practices described in this Special Section.

## SPECIAL SECTION "B"

### Cybercrimes, unlawful data processing and offences concerning violations of copyrights

**1. Types of Cybercrime (art. 24-bis of Decree)**

Law n. 48 of 2008 ratified and implemented the Council of Europe Convention on Cybercrime, Budapest, 23 November 2001.

Law n. 48 introduced in the criminal code new types of crime.

At the same time, it introduced in the Decree the art 24-*bis*, that established the entities' administrative liability in the event of cybercrimes committed in their interest or to their advantage.

The content of the regulation is the following: "*(Cybercrimes and unlawful data processing). – 1.* In relation to the commission of the offences referred to in articles 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* and 635-*quinquies* of the criminal code, a monetary sanction is applicable ranging from 100 to 500 quotas. *2.* In relation to the commission of the offences referred to in articles 615-*quater* and 615-*quinquies* of the criminal code, a monetary sanction is applicable not exceeding 300 quotas. *3.* In relation to the commission of the offences referred to in articles 491- *bis* e 640-*quinquies* of the criminal code, with the exception of the provisions contained in article 24 of the present decree referring to computer fraud against the State or another entity, monetary sanctions of up to four-hundred shares are applied. *4.* In the case of a conviction for one of the offences indicated in paragraph 1 the disqualification sanctions contained in article 9, paragraph 2 letters *a)*, *b)* and *e)* are applied.

In the case of a conviction for one of the offences indicated in paragraph 2 the disqualification sanctions contained in article 9, paragraph 2 letters *b)* and *e)* are applied. In the case of a conviction for one of the offences indicated in paragraph 3 the disqualification sanctions contained in article 9, paragraph 2 letters *c)*, *d)* and *e)* are applied".

The following is a short description of the offences referred to in this regulation. .

*Unlawful access to computer system (art. 615-ter p.c.)*

This provision punishes the conduct of whoever accesses illegally or without authorization a computer system protected by security measures.

*Unlawful interception, obstruction or interruption of computer communications (art. 617-quater p.c.)*

This rule concerns whoever fraudulently and on purpose intercepts, obstructs or interrupts computer communications.

*Installation of equipment designed to intercept, prevent or interrupt computer or telematic communications (art. 617-quinquies)*

This regulation anticipates the protection of confidentiality of telematics communication and punishes the mere installation of equipment designed to intercept communications, even when no interception or interruption is actually performed.

*Type of damage (635-bis – 635-quinquies p.c.)*

Articles 635-bis and following sections punish a series of types of offences having in common behaviours aimed to damage data and computer systems.

Article 635-bis, punishes the damage to computer data and computer programs. The provision punishes whoever damages, destroys, degrades, deletes, alters or suppresses third-party information with imprisonment from 6 months to three years.

Article 635-ter punishes the conduct of whoever commits a fact in order to destroy, damage, cancel, alter or remove information, data or computer programs used by the State or other public body or pertaining thereto, or however of public interest.

Article 635-quarter punishes the damage to computer or telematics systems and, in particular, who adopts one of the conducts set out in article 635-bis aimed at damaging programs and data, and more generally, damages the functioning of an entire IT system.

Article 635-quinquies punishes ever more seriously the facts referred to in the article above if against systems of public utility.

*Abusive detention and dissemination of access codes to computer or telematic systems (art. 615-quater p.c.)*
This law punishes anyone who, with the purpose of procuring gain for him/herself or for others, or of causing damage to others, illegally acquires copies, circulates, communicates or hands over codes, passwords or other means of access to protected computer or information systems.
*Diffusion of equipment intended to damage or disrupt a computer system (art. 615-quinquies p.c.)*
This law punishes anyone who spreads computer viruses, or programs intended to access and damage computer systems and contained data.
*Forgery of electronic documents (art. 491-bis p.c.)*
this crime extends the criminal prosecution of the offences provided for in the heading "misrepresentation in deeds" , if their subject-matter is an "electronic document.

*Computer fraud of the subject providing electronic signature certification services (art. 640-quinquies p.c.)*
This article punishes the subject poviding electronic signature certification services, if the latter in order to obtain an unjust profit for oneself or for others or cause damage to others, violates the obligations established by law for issuing a qualified certificate.
As regards the copyright laws, the Law 99/09, 23 July 2009, "Provisions for the development and internationalisation of businesses, as well as energy", introduced in the Legislative Decree 231/01 the following regulatory provision:
(*"Offences concerning violations of copyrights"*) in relation to the commission of offences referred to in articles 171, primo paragraph, letter a-bis), and third paragraph , 171-bis, 171-ter, 171- septies ad 171-octies of the law 22 April 1941, n. 633, a monetary sanction is applicable to the entity not exceeding 500 quotas.
2. In the event of conviction for offences referred to in paragraph 1 the disqualification sanctions referred to in article 9, paragraph 2, are applied for a period of no more than one year.
Without prejudice to the provisions of art. 174- quinquies of law n. 633, 1941.
Below is a short description of the offences referred to in this regulation.
*Dissemination, in whole or in part, of a protected intellectual work by telematics network (art. 171, i paragraph, letter a-bis of law 633/1941)*
This offence is committed when a person violates the copyright, by spreading – through telematics networks – in whole or in part, intellectual work.
*Illegal handling of protected database and computer programs (art. 171- bis of law 633/1941)*
This offence is committed when a person, in order to earn profits, illegally duplicates, imports, disseminates, sales, leases, spreads/transmits, holds for commercial purposes – or in order to gain profit – protected databases and computer programs.
*Illegal handling of literary, music, multimedia, cinematographic, artistic works (art. 171- ter law 633/1941)*
This offence is committed when a person, for profit purposes, duplicates illegally, imports, disseminates, sales, leases, spreads/transmits, holds for commercial purposes – or in order to gain profit – any work protected by copyright, including literary, music, multimedia, cinematographic, artistic works.
*Improper handling of media not subject to labelling requirements (art. 171-septies law 633/1941)*
This offence is committed when manufacturers or importers of media not subject to the SIAE identification mark do not inform the SIAE within thirty days from the date of commencement of trade in Italy or from the date of importation of the data required for the unique identification of said media, or when they falsely states that they have fulfilled their labelling obligations.
*Illicit or fraudulent handling of decoding devices for conditional access audiovisual transmissions (art. 171- octies della law 633/1941)*
This offence is committed when, for fraudulent purposes, a person fraudulently produces, places for sale, imports, promotes, installs, modifies, uses for public and private apparatuses or parts of apparatuses, acts of decoding audio-visual transmissions with conditioned access executed via air, satellite, or cable, in either analogical or digital form.

**2. At-risk areas**

Any activity that implies access to the IT network shall be considered- even theoretically - at risk-areas.
Considering the specific types of crime at issue, the illicit activities that might involve TAGETIK SOFTWARE S.R.L. or its subsidiaries are:
- alteration or falsification of public or private electronic documents;
- espionage or sabotage activities by computer against public or private competitors (creation, modification, alteration of third-party data; unauthorised access to third-party systems; unauthorized modifications to third-party programs; illegal possession of third-party systems' access *password;* illicit interception of third-party computer communications; installation of equipment designed to carry out this illicit activity; spread of viruses… ).
- distribution of software without the required licenses and violation of the copyright laws

Since TAGETIK SOFTWARE S.R.L. mainly operates (and almost exclusively) in the IT sector and in direct contact with Databases and, more generally, with the clients' IT structure, the likelihood of these offences being committed has been assessed as significant following the analysis and mapping of risks.

**3. Rules of conduct and procedures**

All Addressees:
- must use the company's IT network exclusively for professional purposes, operations and communications;
- can use third party IT networks only for professional purposes;
- shall protect clients' data they can access for activities development reasons and must maintain the strictest confidentiality according to the confidentiality agreements stipulated with the client company, also after termination of the commercial relations with the client.
- shall protect the IT tools, company data, clients' data as well as laptops and mobile devices
- must avoid using software and computer programs in violation of the copyright laws
- must notify the Head of IT and/or the Management of any event or anomaly that might indicate possible computer crimes

The prevention of the offences referred to in this Special Section can and must be based on three key points:
- identification of the persons who access and use the IT network;
- suitable measures intended to protect network access by third parties, in order to prevent anyone from acting anonymously on the company's IT network.
- periodical check of the lawfulness of the software installed on PCs and on the company's IT network

It is worth noting that TAGETIK SOFTWARE S.R.L. has a Document on Security and has adopted an Information Security Management System in accordance with UNI CEI ISO/IEC 27001:2013 (certificate issued by the third party Organization DEKRA CERTIFICATION S.r.l.) providing the security measures aimed at preventing illicit access (physical or computer) to sensitive data handled by the company: the Special Section refers to such measures that are thus considered part of this Model.
Moreover, Chief executive officers have been entrusted with data protection tasks in the consultancy and software development areas.

**4. Internal reference procedures and documents**

I With regard to this special section, the following internal documents and procedures are available:

- All the ISMS procedures and documents in accordance with UNI CEI ISO/IEC 27001:2013
- Security Policy Document
- Company IT regulations

These procedures and documents complete the practices described in this Special Section.

## SPECIAL SECTION "C"

### Corporate crimes

**1. Introduction**

The Legislative Decree n. 61, 2002 reformed the regulations concerning the corporate crimes by reformulating articles 2621 and ss. c.c. The decree introduced the article (art. 25-*ter*) that extended the possibility of establishing the administrative liability of the Entities also in the event of "offences in the corporate sphere provided for by the Civil Code, if committed in the company's interest, by directors, chief executives or liquidators, or by persons subject to their supervision, where the act would not have been committed if they had exercised supervision in conformity with the legal obligations inherent in their position"

**2. Types of Corporate Crimes**

The following is a short description of the main crimes that are relevant for the purposes of this Second Special Section.

*2.1 FRAUDULENCE*

*Misleading corporate statements (art. 2621 and 2622 c.c.)*

The offences referred to in articles 2621 and 2622 c.c. are represented by the conduct of administrators, general managers, auditors and liquidators provide false information or omit information, misleading the addressees of such communications.

The conduct, for it to be subject to criminal sanction, must have the purpose to mislead shareholders, creditors or the public on one hand, and on the other hand to obtain a benefit personally or on behalf of other persons.

*False Prospectus (art. 2623 c.c.)*

The regulation referred to in article 2623 concerns the protection of the truthfulness and completeness of information addressed to the market, in those cases where the company wants to solicit investment or wants to be listed on the stock market, or obtain public share exchange or purchase offers. Indeed, the law punishes those who spread false information or conceals true information with the purpose to mislead the public.

As in the previous case, the conduct, for it to be subject to criminal sanction, must have to purpose to mislead the addressees on one hand, and on the other hand to obtain a benefit personally or on behalf of other persons.

This conduct constitute a criminal offence if it results in a financial damage to the addressees of the prospectus.

*Falsehood in reports and in notifications from audit companies (art. 2624 c.c.)*

This protects the truthfulness and completeness of the notifications from audit companies.

As in the previous case, if the conduct results in a financial damage to the addressees, the sanction is aggravated and the offence becomes crime.

The offence referred to in article 2624 is considered a crime because it can be committed by auditors; this does not mean that the administrators and all other entities listed under art. 25-*ter* of the Decree cannot be involved under the title of accessories to the commission of the offence

*2.2 PROTECTION OF SHARE CAPITAL*

*Undue repayment of contributions (art. 2626 c.c.)*

This constitutes the conduct of directors who, except for cases of legitimate reduction of share capital, repay, including with simulation, contributions to the shareholders or free them of the obligation to effect them.

*Unlawful distribution of profits and reserves (art. 2627 c.c.)*

Distribution of profits and reserves on profits not actually realised or destined by law to reserve, or distribution of reserves which cannot be distributed by law.

Nevertheless, the provision stipulates that returning the profits or re-establishing the reserves before the time limit specified for approval of the financial statements extinguishes the offence.

*Unlawful transactions on shares, listed shares or of the parent company (art. 2628 c.c.)*

Acquisition or subscription of shares or treasury shares, causing damage to the wholeness of the share capital or the reserves not distributable by law

It should be noted that re-establishing the share capital or the reserves before time limit specified for approval of the financial statements extinguishes the offence.

*Transactions to the detriment of creditors (art. 2629 c.c.)*
This guarantees the creditors and prohibits reduction of capital, merger with other companies or demergers, causing damage to the creditors.
It should be noted that the payment of compensation for damages to the creditors, prior to a court ruling, extinguishes the Offence
*Omission of notification of conflict of interest (2629 bis c.c.)*
Provision introduced by L. 262/2005 providing the "Dispositions for the protection of savings and the discipline of financial markets"
Art 2629 *bis* of the Civil Code concerns the violation of article 2391, 1 paragraph, c.c. (that establishes the obligation to notify the conflict of interest) by administrators of companies with shares committed to trading on regulated markets or with a significant portion held by public investors, or subject to supervision in accordance with TUF.
*Fictitious formation of capital (art. 2632 c.c.)*
The regulation covers three types of conduct, all resulting in the formation of fictitious capital:
- allocation of shares or capital shares for an amount lower than their par value;
- mutual underwriting of shares or stock;
- considerable overpricing of assets in kind, credits, or the assets of the company in the case of transformation.

*Unlawful distribution of company assets by liquidators (art. 2633 c.c.)*
This concerns the conduct of liquidators who cause damages to creditors, by allotting the corporate goods among the partners before the payment of companies' creditors or allocating sums necessary to pay them
The payment of compensation for damages to the creditors, prior to a court ruling, extinguishes the Offence

*2.3 SAFEGUARD OF CORRECT OPERATION OF THE COMPANY*
*Prevented control (art. 2625 c.c.)*
The offence consists impeding the carrying out of the control or auditing activities legally assigned to the shareholders, other corporate bodies, or auditing firms by concealing documents or with other appropriate tricks.
If actual damage is caused, a more serious punishment applies.
*Bribery among private individuals (art. 2635 c.c.)*
The offence consist in providing sums of money and/or benefits (even just promised) resulting in the violation of the duty of loyalty and damaging the company.
*Unlawful influence on the meeting (art. 2636 c.c.)*
This provision punishes the conduct of whoever, by means of simulated acts of by fraud, has an illegitimate influence on the formation of the assembly majority, in order to obtain a benefit personally or on behalf of other persons.

*2.4 PROTECTION AGAINST FRAUD*
*Market manipulation (art. 2637 c.c.)*
The offence under article 2637 occurs when untrue information is circulated or simulated transactions or other expedients are utilised, with the specific intention to cause a significant change in the price of financial instruments which are not quoted or for which no application for listing on a regulated stock exchange has been presented, or with the objective of significantly influencing the public opinion in regard to the financial stability of the banks or banking groups.
It should be noted that law, in force since 2005, punishes only the market manipulations that affect the value of unlisted securities. Indeed, since that year, the legislator introduced articles 184 and 185 in the TUF, regulating the market abuse on securities of listed companies. The same law introduced the new article 25 *sexies* in the Decree, establishing the corporate liability of the Entities also for this type of offence.

*2.5 SAFEGUARD OF PUBLIC SUPERVISOTY AUTHORITIES*
*Obstruction to the activities of public supervisory authorities (art. 2638 c.c.)*
This offence occurs in two cases that differ in terms of conduct and context.
The first case occurs on the one hand when including untrue facts, even though subject to assessment, on the economic, asset or financial situation of the individuals under surveillance, in the communications provided by law

to the Public Surveillance Authorities, on the other hand when concealing facts that should have been communicated regarding such economic, asset or financial situation.
The second case concerns any other form of obstruction – wittingly committed - to the activities of Public Supervisory Authorities.

## 3. At-risk areas

In view of the offences and conducts described above, the analysis of TAGETIK SOFTWARE S.R.L.'s business activities showed a low risk of such corporate crimes being committed.
Indeed TAGETIK SOFTWARE S.R.L. is not a listed company, does not resort to public investors, is not supervised by the Public Supervisory Authority (CONSOB).
The risk of corporate crimes is connected to those crimes involving any legal person that carries out business activities. The following areas are involved:
A) direct communications to shareholders or to the general public and preparation of the financial statements; it should be noted that in this case the shareholders are also the administrators, therefore the risk of this offence being committed is very low.
B) operations affecting the share capital and management of the *corporate governance*;
C) commercial promotion activities and management of trade relationships, also between private entities
The list could be integrated in the future with more at-risk areas (with the subsequent definition of rules of conduct and procedures).
The Supervisory Body can submit to the Board of Directors modifications to the text of this Special Section.
However, the Board of Directors can autonomously take similar initiatives.

## 4. General Rules of Conduct

All addressees must:
- behave in a honest, transparent and collaborative manner, in compliance with the laws and the company's procedures, in all the activities related to the preparation of the financial statements and other corporate communications, in order to provide shareholder and third parties with truthful, complete and correct information about the financial and economic situation of TAGETIK SOFTWARE S.R.L.;
- comply with the laws and internal procedures aimed at safeguarding the integrity and consistency of the share capital, in accordance with creditors and third party requirements;
- safeguard the function of TAGETIK SOFTWARE S.R.L.'s company bodies, by supporting any form of control of the corporate management and encouraging the Shareholders' Meeting to express its will freely;
- promptly and accurately provide communications in accordance with the applicable law, avoiding any obstacle to the auditors' activities;
- not disseminate information about initiatives and selection of trade partners (conclusion of agreements by TAGETIK SOFTWARE S.R.L., collaboration with the Corporation, etc.), unless where strictly necessary and upon approval from the partner itself.
- adopt ethical practices in commercial dealings in order to avoid bribery among private individuals

## 5. Particular rules of conduct related to the specific at-risk areas

### 5.1 Communications to Shareholders and to the public

*Financial Statements and other corporate communications*
TAGETIK SOFTWARE S.R.L. has defined a specific procedure for the management of its financial statements and has identified the functions involved in such activities.
Involved functions:
- group administrators;
- Italian and foreign companies administrators;
- external tax consultant.

The Company has adopted also a scrupulous internal control system aimed at monitoring, in real time, the statement of account of TAGETIK SOFTWARE S.R.L.

**5.2 Safeguard of Share Capital**

Any operation that, even indirectly, might affect the share capital of TAGETIK SOFTWARE S.R.L., such as the purchase or sale of shareholdings or company branches, merger, demerger or spinoff, shall include:

- allocation of decision-making and executive responsibilities, as well as the coordination among the corporate functions;
- provision of information to the Supervisory Body in order to enable it to follow the entire decision- making process;
- provision of the documentation of each project to the Supervisory Body;

As regards the possible conflict of interest, the administrators must provide the Board of Directors and the Supervisory Body with all the information concerning their appointments or participations they hold, directly or indirectly, in other companies - as well as the related termination or modification – that might lead to a conflict of interest in accordance with article 2391 c.c.

**5.3 Relations with the Competent Authorities**

Three fields of activity are considered relevant with regard to the relations with the competent Authorities:

- transmission of information required by law and regulations;
- transmission of information required by the Competent Authorities;
- rules of conduct in the event of inspections by the Authorities.

The principles below shall be followed:

- terms and means of transmission and of the internal circulation of necessary data for the preparation of the information required by the competent Authorities, and definition of procedures aimed at guaranteeing the highest truthfulness and completeness of data;
- designation of the persons responsible for ensuring compliance with the procedures and providing a statement of truthfulness and completeness of the provided information;
- in case of inspection, cooperation of all departments, designation of a person responsible for all the necessary activities, for coordinating the involved departments and providing the information required by the supervisors;
- possibility for all managers to consult the Supervisory Body about the activities connected the relations with the competent Authorities and report any flaws in the procedures and operational methods;
- the person appointed to ensure cooperation in the event of inspection, shall prepare a report for the Supervisory Body on the investigation that will have to be periodically updated according to the related developments and results.

## 6. Internal reference procedures and documents

With regard to this special section, the following internal documents and procedures are available:

1. Code of Ethics
2. Financial Statements preparation procedure
3. Commercial procedure

These procedures and documents complete the practices described in this Special Section.

## SPECIAL SECTION "D"

### Market abuse

### 1. Crimes referred to in articles 184 and 185 TUF (art. 25 sexies of Decree)

Article 9, law 18 April 2005, n. 62, implementing directive 2003/6/CE of the European Parliament and of the Council of 28 January 2003, introduced article 25-*sexies* in the Decree. This provision extends the scope of regulation of the administrative responsibility of the corporate body to behaviours to include conduct involving market abuse.
Indeed, the same law reshaped the framework of the market abuse crimes, introducing articles 184 and 185 in the TUF.
Article 184 punishes the insider dealing with imprisonment from two to twelve years and with a fine from € 40.000 to € 6,000,000: the crime occurs when a member of administrative, management or auditing bodies possessing inside information 1) carries out transactions in regard to financial instruments by using such information or 2) discloses such information to third parties or 3) encourages or induces other parties to carry out similar transactions.
According to paragraph 2 of the law, the same crime can be committed by whoever comes into possession of sensitive information with the purpose to commit an offence.
Moreover, article 181 of TUF defines the concept of inside information: information which has not been disclosed, concerning either directly or indirectly one or more financial instruments issuers, and which, if made public, could have a significant effect on the prices of such financial instruments.
Information can be considered to be precise if: i) It refers to a complex of existing circumstances or to circumstances that may reasonably be expected to exist or to an event that has taken place or that can reasonably be expected to take place; ii) is sufficiently specific to allow conclusions to be drawn as to the possible effect of the complex of circumstances or the event described in point a) on the prices of the Financial Instruments.
Information which, if made public, could have a significant effect on the prices of Financial Instruments means: information that a reasonable investor would presumably use as one of the elements on which to base his or her investment decisions.
Article 185 of TUF punishes market manipulation.
This law punishes with imprisonment from two to twelve years and a fine from € 40.000 to € 10.000.000 three types of conduct:
1) spreading of false rumours;
2) performance of fictitious transactions;
3) other tricks
If such conducts provoke a notable alteration of the price of financial instruments.

### 2. At-risk areas

TAGETIK SOFTWARE S.R.L. is not a listed company: this aspect eliminates the risk of market abuse involving securities of the company. Moreover, TAGETIK SOFTWARE S.R.L. has no equity investments in any listed company and does not operate in the stock market.
On the contrary, the management of information related to listed client companies shall be considered an at-risk area: TAGETIK SOFTWARE S.R.L.'s consultants have direct access to data relating to financial statements and/or group consolidations of companies listed in the Italian and foreign stock exchange.
The company's areas considered to be mainly at risk are the following:
a. management of information relating to any relationships with listed clients or connected to other listed entities, before their formalisation;
b. spread of information related to new agreements, new services and new partnerships involving listed clients or connected to listed third parties.

### 3. General rules of conduct

All information relating to the company's management, the clients, financial statements data, agreements, etc. must be considered confidential and shared only with the persons involved in the project activities.
With reference to the consultancy activities, TAGETIK SOFTWARE S.R.L. provides the following rules of conduct:
- any communication with third parties must follow the principles of confidentiality;

- all consultants involved in projects during which they will have access to inside information will have to sing a confidentiality agreement and an agreement concerning the protection of client's data;
- all Addressees must promptly report any behaviour that could imply improper use or disclose of confidential information, or market abuse.

**6. Reference internal procedures and documents**

With regard to this special section, the following internal documents and procedures are available:

1- Code of Ethics
2- Consulting Procedure
3- HR Procedure

These procedures and documents complete the practices described in this Special Section.

## SPECIAL SECTION "E"

### Offences committed in breach of occupational health and safety regulations

**1. Manslaughter and grave or very grave negligent personal injury, committed in violation of occupational health and safety regulations (art. 25 septies of Decree)**

Article 25-*septies* of the Decree, introduced by Law 23 August 2007 n. 123, ad replaced by article 300 of Legislatove Decree 81/2008 (Consolidated Law on the protection of health and safety in the workplace), has extended the corporate administrative liability to crimes of manslaughter and grave or very grave personal injury, committed in violation of occupational and safety regulations.

It should be noted that the decree, besides reshaping and reorganizing the legislation regarding the occupational health and safety regulations, has extended the corporate administrative liability and has introduced specific regulations regarding the preparation of the Model.

*Voluntary Manslaughter (art. 589 p.c.)*

Anyone who causes by negligence the death of a person is punishable with imprisonment from six months to five years. If the crime is committed as a result of a violation of road traffic laws or laws for the prevention of occupational accidents, the penalty is imprisonment from two to seven years. In cases of the death of more than one individual or of the death of one or two individuals and injuries to one or two individuals, the penalty is the same as the most severe that can be applied for the violations in question increased by up to a third, although the penalty must not exceed 15 years.

*Personal injury through negligence (art. 590 p.c.)*

Anyone who causes by negligence the injury of another person is punished with imprisonment for up to three months or a fine of up to € 309.

If the injury is serious, the offence is punished with imprisonment from one to six months or a fine from € 123 to € 619; if it is very serious, it is punished with imprisonment from three months to two years or a fine from € 309 to € 1.239.

If the crimes referred to in paragraph two above are committed as a result of violations of road traffic laws or laws for the prevention of occupational accidents, the penalty for serious injury is imprisonment from three months to a year or a fine from € 500 to € 2,000, the penalty for very serious injury is imprisonment from one to three years.

When more persons are involved, the penalty that is inflicted for the most serious of the committed violations is applied, increased up to three times; but imprisonment cannot exceed five years.

The offence is punishable on complaint by the injured party, unless any of the circumstances referred to in subparagraph one or two occur, limited to acts committed in violations of occupational accident prevention regulations that causes an occupanional disease.

*****

It should be notet that not all cases of voluntary manslaughter or serious or very serious personal injury through negligence imply administrative liability: according to article 25-*septies*, administrative liability is implied only when the negligent conduct that caused injury to someone is due to failure to comply with one or more laws and regulations protecting health and safety at work.

Furthermore, it should be noted that, according to article 583 paragraph 1, personal injury should be considered "serious" if: (i) it causes an illness which endangers the life of the injured person, or an illness or incapacity to attend to the normal activity for a period exceeding forty days; (ii) If the event results in the permanent weakening of a sense or an organ.

According to article 583 paragraph 2, the injury is considered "very serious" if the event results in: (i) an illness that is certainly or probably incurable; (ii) the loss of a sense; (iii) the loss of a limb or mutilation that renders the limb useless, or the loss of the use of an organ or a permanent and serious difficulty of speech; (iv) the deformation or permanent disfigurement of the face.

As regards the penalty provisions introduced by the Decree, three levels of severity of the offence are distinguished. In particular:

(i) in the event of involuntary manslaughter caused by the most serious infringements referred to in article 55 paragraph 2 of the Consolidation Act (failure to write or drafting of incomplete risk assessment document

required by the law in companies where business activities are at high risk), the fine is 1000 quotas; the interdiction measures ranges from three months to one year;
(ii) in the event of involuntary manslaughter committed in violation of occupational health and safety regulations, the fine ranges from 250 to 500 quotas; the interdiction measures range from three months to one year;
(iii) in the event of serious or very serious negligent injury, the fine cannot exceed 250 quotas; the interdiction measures cannot exceed six months.

*****

**2. Addressees**

In view of the purposes of the case under review, it is evident that any activity represent a risk for those who perform it as well as for the wider community.
Therefore, the addressees of this special section, in addition to the addressees of the Model, are:
- all those with responsibilities related to health and safety at the work place (e.g. employer's proxies, sfety officer, company doctors, emergency workers, etc.);
- external service provides working within the company areas;
- contracting companies' workers;
- other collaborators, even occassional;
- visitors.

**3. Purposes of this special section**

First, it should be noted that the offences described in this Special Section, unlike all the others referred to in the Decree, do not result from voluntary unlawful conducts but from mere neglicence.
In the event of unintentional injuries, it is due to an unintentional failure to comply with the accident prevention regulations and is not committed with criminal intent.
The purpose of this Special Section is to prevent these types of crime through a series of internal organisational measures aimed at guaranteeing compliance with the occupational health nd safety regulations imposed by law.
In accordance with article 30 of the Legislative Decree 81/2008, the Organisational Model, with regard to the specific offences referred to in article 25-septies, should adhere to the following principles:
a) compliance with the technical-structural standards prescribed by the law in regard to the plant, premises and work equipment;
b) risk assessment and preparation of the ensuing prevention and protection measures;
c) activity of an organisational nature such as, first aid, contract management, periodic meetings concerning safety matters, consultation with the workers' safety representative;
d) activities of health surveillance;
e) worker information and training;
f) supervisory activity, in regard to the observance by the workers of the occupational safety procedures and instructions;
g) acquisition of mandatory documents and certificates required by law;
h) periodic verification of the application and effectiveness of the procedures adopted.
On the other hand, it should be noted that in the specific context of TAGETIK SOFTWARE S.R.L., whose structure basically consists of offices and workers that mainly carry out intellectual activities, the risk of offences set out in article 25-septies being committed is very low even though, obviously, it cannot be completely excluded.
Therefore, this Model is intended to:
- provide measures and methods aimed at monitoring the implementation of the activities provided by the Legislative Decree 81/2008 as further amended and extended in relation to the mandatory requirements for TAGETIK SOFTWARE S.R.L.;
- provide for the extension of the existing disciplinary system.

**4. Parties involved in safety-related tasks**

Those parties playing a significant role for the protection of safety and health in the workplace are:
1. Employer, for those duties that are not delegable;
2. Occupational Health and Safety Officer;
4. First aid and fire prevention officers;
5. Safety rules sueprvisors;
6. Workers' health and safety representative;
7. Company Doctor;
8. Workers.

The employer for the purposes of responsibility for employees safety and health at work is one of the Company's Managing Directors and has been appointed by the Board of Directors. He/she is responsible for assessing the risks and appointing the Occupational Health and Safety Officer –currently is an external consultant that took up the assignment on a personal basis.
The First aid and fire prevention officers have been have been appointed and have then attended the related training and/or refresher courses; a Company doctor has been appointed as well.
This list includes also all workers: the contribution of their kkowledge regarding the security related risks is essential for an internal system that aims at protecting the safety at work.

**5. System planning and organisation**

In order to actually implement the security management principles, TAGETIK SOFTWARE S.R.L. has adopted specific health and safety in the workplace management system in accordance with the interntional law BS OHSAS 18001:2007 and certified by the DEKRA CERTIFICATION S.r.l. third-party body.

**6. Risks assessment**

An essential prerequisite for an efficient prevention of occupational risks is an effective, suitable and ongoing assessment of the workplace health and safety risks.
This resulted in the Risk assessment document in accordance with the Consolidated Law. It is written, updated and perfected by the Employer, with the support of the Occupational Health and Safety Officer.
In addition to this document there are more specific documents, conserning specific types of risk, such as the fire risk assessment and the work-related stress risk.
On the basis of the results of the workplace health and safety risks assessment, TAGETIK SOFTWARE S.R.L. has implemented the necessary risk reduction measures aimed at preventing the occupational diseases and has adopted the procedures defined in the health and safety management system.
The assessment of possible health risks is also very important. In this case, the role of the Company Doctor and the medical records are essential. The health documentation is kept in company archives in accordance with the privacy laws.
Every year the Company Doctor writes a report containing particular diseases or injuries occurred in the previoues year.

**7. Exceptionald and/or extraordinary cases**

An effective prevention should be based not only on the analysis of the ordinary activities, but also on extraordinary cases and circumstances: cases involving persons that do not directly belong to the company or, broadly speaking, emergency situations that imply risky activities or a lowering of the prevention measures level.
Thi is why TAGETIK SOFTWARE S.R.L. has regulated also the health and safety protection measures in case of tenders assigned to third parties.

**8. Information and training**

It is also important to provide all employees and other involved parties with the propert training and information on workplace health and safety.

TAGETIK SOFTWARE S.R.L., with the support of the Occupational Health and Safety Officer, defines the measures to guarantee:
1. effective information and training for workers and all parties involved in the company activities;
2. contribution of the knowledge and experience of the workers daily involved in the company activities.
As regards the first point, the following activities have been regulated:
- periodic or specific mass training;
- individual training for new employees and in the event of change of job;
- free access to the safety documentation.
As regards the second poinr, TAGETIK SOFTWARE S.R.L. provides information and training activities that must be documented by a specific form signed by the employee.
- periodic meetings with the employees and their representatives;
- report of malfunctions or lacks.
The reports can be submitted to the Occupational Health and Safety Manage.

**6. Internal reference procedures**

With regard to this special section, the following internal documents and procedures are available:

1- Workplace safety and health management system procedures in accordance with a BS OHSAS 18001;2007.
2- Company Risks assessment document (and workplace health and safety documents)

These procedures and documents complete the practices described in this Special Section.

## SPECIAL SECTION "F"

### Crimes of Receiving of Stolen Goods, Money Laundering and Utilisation of Money, Goods or Benefits of Unlawful Origin and self-laundering

Offences referred to in article 25–octies have been instroduced in the Legislative Decree 231/01 by the Legislative Decree 21 November 2007, n. 231 "Implementation of directive 2005/60/CE concerning prevention of the use of the financial system for the purpose of money laundering and of financing terrorism, and directive 2006/70/CE which prescribes the measures for implementation". The Decree n. 231/2007 is intended to prevent the financial system from being used for the purposes of money laundering or the financing of terrorism.
Penalties of both a monetary nature and consisting of prohibitions are applicable quotas.
The monetary sanction ranges from 200 to 1000 quote.
In the event of conviction for the crime, the entity is punished with the interdictive sanctions prescribed by article 9, paragraph 2° of Legislative Decree 231/2001 for a period not exceeding two years.

*Handling stoles goods (art. 648 P.C.)*

This offence occurs when any person, for the purpose of obtaining a personal profit or for others, purchases, receives or conceals money or goods deriving from any crime whatsoever, in whose commission he did not participate, or in any case concurs in their purchase, receipt or concealment.
This crime implies the specific malice by the person who acts, in other words, the knowledge and intention of gaining a profit, for himself/herself or for others by purchasing, receiving or concealing the goods of illegal origin.
Moreover it implies the knowledge of the criminal provenance of the money or of the good; the existence of this psychological element could be acknowledged in case of serious or unique circumstances – such as, the qualities and characteristics of the good, the unusual economic and contractual conditions of the operation, the condition or the job of the owner of the assets – proving that the actor knew the origin of the asset or of money.

*Laundering (art. 648 bis P.C.)*

This crime occurs when the actor, who did not contribute to the commission of the infringement, replaces or trasfers money, goods or other utilities deriving from intentional criminal acts, or carries out other transactions in their regard, in order to prevent the identification of their criminal provenance.
The law is intended to punish whoever – aware of the criminal provenance of money, goods or other utilities – perform these operations, peventing the identification of the criminal provenance of such assets.
Having acted for obtaining a personal profit or helping the offenders in order to obtain profit is not necessary for the purposes of completion of the crime.

*Utilisation of Money, Goods or Benefits of Unlawful Origin (art. 648 ter P.C.)*

The criminal behaviour occurs when using money, goods or benefits of unlauful origins in economic and financial activities, except for the cases of concurring in crime and the cases provided for in articles 648 (receiving stolen goods) and 648 bis (lundering) P.C..
Unlike the money laundering offence, article 648 ter limits the conduct to the use of such resources in financial and economic activities.

*Self-laundering (art. 648 ter-1 P.C.)*

The article punishes the conduct of who, having committed or contributed to an intentional criminal act, replaces, transfers or uses, in economic and financial activities, money, goods or other utilities originated from the commission of such crime, so as to prevent the identification of their criminal provenance". The sanction is imprisonment from 2 to 8 years and a fine from € 5.000 to € 25.000. Imprisonment is reduced from 1 to 4 years if the predicate offence is punished with imprisonment not exceeding 5 years.
The penalty is higher if the facts are committed while carrying out banking, financial or other professional activity; the penalty is reduced if the person acted in order to "avoid additional consequences or to ensure evidence of the crime and the identification of goods, money and other utilities of unlawful origin.".
Self-laundering is not punished "when money, goods or other utilities are are for personal use" as long as purché there was no intention to conceal the assets derived from the offence.
The self-laundering regulations do not apply to those who dhere to the "voluntary disclosure" procedure, namely voluntarily contributes to repatriating funds illegaly held abroad.

## 2. Purpose of this special section

La presente parte speciale refers to kinds of conduct engaged in by the Corporate Bodies and employees, and also by consultants, as more fully discussed in the General Section, who are involved in the various classes of Sensitive Activities.
The object of this Special Section is to ensure that the people identified above should maintain conducts in conformity with the reference principles set out below, in order to prevent the commission of the offences indicated in the previous paragraph.
This special section identifies the reference principles for the definition of the Model, in relation to the specific sensitive activities in order to prevent the "self-laundering" offence from being committed.

## 3. General reference principles

Employees and Corporate bodies must comply with:

- Internal control system, corporate procedures, documentation and provisions relating to the organisational and corporate hierarchical/functional structure;
- Disciplinary system;
- Applicable law.

## 4. General behaviour principles

This section prohibits the Corporate Bodies and the employees of Tagetik Software to:

- Implement behaviours that, individually or collectively, may lead, directly or indirectly, to the offences referred to in article 25-octies of the Legislative Decree 231/2001 (self-laundering);
- Breach the corporate principles and procedures applicable to this special section.

## 5. Sensitive activities in relation to the self-laundering offence for the purposes of Legislative Decree 231/2001

The sensitive activities identified in relation to the self-laundering offence referred to in article 25-octies del D.Lgs. 231/2001, are:

- COMPANY PERFORMANCE AND OPERATIONS MANAGEMENT
- MANGEMENT OF ADMINISTRATIVE AND ACCOUNTING PROCESSES AND FINANCIAL FLOWS

It should be notet that, in addition to these activities, other voluntary predicate offences could lay behind the self-laundering offence in accordance with Legislative Decree 231/01 (e.g. corruption, solo a titolo di esempio si pensi alla corruzione, fraud to the detriment of the State, commercial fraud, infringements of intellectual and industrial property rights, etc.).

## 6. General control principles

The general control principles can be summarized as follows:

- SEGREGATION OF DUTIES: segregation of duties among who authorizes, who implements and who controls;
- EXISTENCE OF PROCEDURES/REGULATIONS/CIRCULARS: company provisions and procedures shall provide the principles of conduct concerning the performance of sensitive activities and the archiving of important documents;
- AUTHORIZATION AND SIGNATORY POWERS: these must be i) consistent with the organisational and management responsibilities assigned; ii) clearly defined and known within the company;

- TRACEABILITY: all operations related to the sensitive activities must be registered. The decision-making, authorization and implementation process must be verifiable, also through documents and the archives deletion or destruction procedure must be regulated.

**7. Corporate obligations and operations management**

The regulation of the activity must follow the reference principles relating to the regulations of the sensitive activities "Share capital operations: management of contrbutions, business assets, revenues and reserves, operations on investments and capital" and "Financial flows management".

**8. Management of administrative and accounting processes and financial flows**

The regulation of the activity must follow the reference principles relating to the regulations of the sensitive activities "Preparation of financial statements, reporting, communication" and "Financial flows management".

**9. Supervisory Body's controls**

The Supervisory Body does not carry out periodic controls on the activities of Tagetik Software S.r.l. in which crimes could be committed, because of the risk assessment performed when preparing and updating the Model.

Nevertheless, the Supervisory Body can access all company's documents relating to Sensitive Activities.

The Supervisory Body shall be provided with concise information in the event of any operation that by virtue of characteristics, size or extraordinary nature, may refer to the profiles described in this chapter, such as:

- Extraordinary company operations;
- Financing activates by partners or third parties of non-banking nature, namely IC financing;
- operazioni sul capitale (es. aumenti di capitale, anche mediante conferimenti);
- other extraordinary operations or financial flows;
- important investment business.

**10. Internal reference procedures and documents**

With regard to this special section, the following internal documents and procedures are available:

1- Code of Ethics
2- Financial statements creation preparation procedure
3- Reimbursment procedures
4- IT purchase procedure
5- Marketing purchase procedure
6- Goods and Services purchase procedure

These procedures and documents complete the practices described in this Special Section.

## SPECIAL SECTION "G"

### Employ of citizens from third countries whose stay is irregular

**1. Crimes referred to in article 22 paragraoh 2 of Legislative Decree 286/1998 (art. 25 duodecies of Decree)**

The legislative decree 109/2012 has extended the list of offences contemplated by the legislative decree 231/01: article 25-*duodecies* contemplating as offence the "*Employ of citizens from third countries whose stay is irregular*".
This crime occurs when an employer who takes on foreign workers without a residence permit referred to in article 22 of legislative decree 286/98 , or whose residence permit has expired and no request has been made in accordance with the terms of the law for a renewal, or whose permit has been cancelled.
Article 25-duodecies exteds the application of the decree to those entities that have employed citizens from third countries whose stay is irregular or has expired, by exceeding the limits set out in the Legislative Decree 268/1998 "Consolidated Act on Immigration" in terms of:

1- Number of employees
2- age
3- working conditions.

The legislative decree 109/2012 provides for punishment set out in article 22, paragraph 12 of the legislative decree 25 July 1998, n. 286:"... An employer who takes on foreign workers without a residence permit referred to in the present article, or whose residence permit has expired and no request has been made in accordance with the terms of the law for a renewal, or whose permit has been cancelled, is liable to a term of imprisonment of between six months and three years and a fine of €5,000 for every worker employed"
The legislative decree n. 109/2012 (published on G.U. n. 172 25 July 2012) has introduced in the Legislative Decree 231/01 the article 25-duodecies "Employ of citizens from third countries whose stay is irregular" with the following text:
"1. In relation to the crime referred to in article 22, paragraph 12-bis, of the legislative decree 25 July 1998, n. 286, a monetary sanction, ranging from 100 to 200 quotas, not exceeding € 150.000 is applicable to the entity "

**2. At-risk areas**

TAGETIK SOFTWARE S.R.L. is a company that applies any labour legislative provision; nevertheless, it has been considered at risk in relation to the article 25-duodecies, because of the significant internationalisation of the company that controls various companies in Third Countries and the presence of personnel that travels and/or comes from various Countries.

**3. General rules of Conduct**

It is forbidden to employ personnel from Third Countries that does not comply with the provisions of the Legislative Decree 286/1998.
Therefore all Tagetik Software S.r.l.'s amployees that come from Third Countries but are resident, even temporary, in Italy with a temporary Residence Permit, shall provide the Human Resources Office with a copy of the permit when hired and upon each renewal.
The Human Resources office shall periodically verify that all employees with temporary Residence Permit comply with the provisions of the Legislative Decree 286/1998

**4. Internal reference procedures and documents**

With regard to this special section, the following internal documents and procedures are available:

1- Code of Ethics
2- HR Procedure

These procedures and documents complete the practices described in this Special Section.