ORGANISATION, MANAGEMENT AND CONTROL MODEL

TAGETIK SOFTWARE S.r.l.

Pursuant to Article 6 of Legislative Decree No. 231/01

Revisions

Rev.	Nature of the revision	Date of Board resolution
0	First issue	20.02.2012
1	General revision	07.11.2017
2	Revision for regulatory update and introduction of Special Part H – Tax Offences	10.10.2022
3	Revision to update paragraph 3.3 of the General Part to incorporate the Whistleblowing procedure following publication in the Official Gazette of Legislative Decree 24/2023 of 10 March 2023, No. 24, "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019"	12.07.2023
4	Revision to update the operating units in Italy and to integrate the UNI EN ISO 14001:2023 environmental management system with the quality and safety management systems. Update of paragraph 3.3 with the insertion of references to the WK SpeakUp policy	22/07/2025
5	Revision to update the composition of the members of the Supervisory Body	22/01/2026

TABLE OF CONTENTS

Section	Page	Rev.
1. Definitions	3	Rev. 4
2. Introduction	4	Rev. 4
3. Organisation and management model	6	Rev. 4
4. Supervisory Body	11	Rev. 4
5. Internal information flows	14	Rev. 4
6. Disciplinary system	16	Rev. 4
7. Dissemination and knowledge of the Model	19	Rev. 4
SPECIAL PART "A" – Relations with the Public Administration	Independent page numbering – total 4 pp.	Rev. 2
SPECIAL PART "B" – Computer crimes and unlawful data processing	Independent page numbering – total 4	Rev. 1

Section	Page	Rev.
	pp.	
SPECIAL PART "C" – Corporate offences	Independent page numbering – total 5 pp.	Rev. 1
SPECIAL PART "D" – Market abuse	Independent page numbering – total 2 pp.	Rev. 1
SPECIAL PART "E" – Offences in breach of occupational health and safety rules	Independent page numbering – total 4 pp.	Rev. 1
SPECIAL PART "F" – Offences relating to receiving stolen goods, money laundering and the use of money, goods or other benefits of unlawful origin, as well as self-laundering	Independent page numbering – total 4 pp.	Rev. 1
SPECIAL PART "G" – Employment of third-country nationals whose stay is irregular	Independent page numbering – total 1 p.	Rev. 0
SPECIAL PART "H" – Tax offences	Independent page numbering – total 2 pp.	Rev. 0

1. DEFINITIONS

TAGETIK (or the Company) — means the company Tagetik Software S.r.l.

Decree — means Legislative Decree No. 231 of 8 June 2001.

Addressees — means all persons required to comply with the requirements set out in the Model, and in particular: all those who act in the name and on behalf of TAGETIK SOFTWARE S.R.L., including directors, statutory auditors, the members of any other corporate bodies, employees, collaborators (including occasional ones), business partners, suppliers, as well as the members of the Supervisory Body.

Entities or Entity — pursuant to Article 1 of the Decree, means entities having legal personality, companies and associations, including those without legal personality, to which the provisions of the Decree apply and, in particular, the administrative liability introduced thereby.

Guidelines — means the Guidelines for the construction of organisation, management and control models pursuant to Legislative Decree 231/2001 published by Confindustria in their most recent revision (March 2014).

Model — means the organisation, management and control model provided for by the Decree.

Predicate Offences — means the offences for which the Decree introduced the administrative liability of the Entity. These are, in particular, the categories of offence identified in Articles 24 and 25 et seq. of the Decree.

Consolidated Act — means Legislative Decree No. 81 of 9 April 2008 (the so-called Consolidated Act on the protection of health and safety in the workplace), as subsequently amended and supplemented.

TUF — means Legislative Decree No. 58 of 24 February 1998, the Consolidated Act on financial intermediation, as subsequently amended and supplemented.

---

2. INTRODUCTION

2.1 The regime of administrative liability of Entities

The alignment of Italian legislation with certain international conventions led, in implementation of the enabling act of 29 September 2000 No. 300, to the enactment of Legislative Decree No. 231 of 8 June 2001, which entered into force on 4 July 2001, "Rules governing the administrative liability of legal persons, companies and associations, including those without legal personality".

The Decree introduced into the Italian legal system the regime of administrative liability of Entities for certain offences (indicated in Articles 24 et seq. of the Decree, the so-called Predicate Offences) committed, or merely attempted, in the interest or to the advantage of the Entities themselves, or of one of their organisational units endowed with financial and functional autonomy, by:

(i) persons who hold powers of representation, administration or management, or who, even on a de facto basis, exercise the management or control of the Entity or of one of its organised units (senior persons within the meaning of Article 5, paragraph 1, letter a) of the Decree); or

(ii) persons subject to the direction or supervision of the persons referred to in point (i) above (persons subject to the direction of others within the meaning of Article 5, paragraph 1, letter b) of the Decree).

The administrative liability of the Entity is direct and distinct from the liability of the natural perpetrator of the offence and is intended to penalise Entities for offences committed to their advantage or in their interest.

By virtue of the liability introduced by the Decree, the Entity is therefore subject to autonomous proceedings and is liable to sanctions which may go so far as to halt its ordinary business activity.

Indeed, in addition to monetary penalties, possible confiscation and publication of the judgment of conviction, the Decree provides that the Entity may also be subject to disqualifying sanctions (Article 9, paragraph 2), such as:

- a ban on carrying on the business;
- the suspension or revocation of authorisations, licences or concessions instrumental to the commission of the unlawful act;
- a prohibition on contracting with the Public Administration, save in order to obtain the performance of a public service;

- exclusion from benefits, financing, contributions or subsidies, and the possible revocation of those already granted;
- a prohibition on advertising goods and services.

Pursuant to Article 4, Entities with their principal place of business in Italy may also be prosecuted for offences committed abroad, where the legislation of the foreign country does not provide for an analogous form of liability.

The administrative liability of the Entity is founded on an "organisational fault": that is to say, the Entity is held administratively liable for the offence committed by its representative if it failed to adopt an organisational structure capable of effectively preventing its commission and, in particular, if it failed to equip itself with an internal control system and with adequate procedures for carrying out the activities most at risk of commission of the offences provided for by the Decree.

Conversely, pursuant to Article 5, paragraph 2 of the Decree, the Entity is not liable if the aforementioned persons acted exclusively in their own interest or in the interest of third parties.

The processes by which such a system of organisation and internal control is to be adopted are set out in Articles 6 and 7 of the Decree, namely:

- the approval, adoption and effective implementation, prior to the commission of an offence, of a Model capable of preventing the commission of the Predicate Offences provided for by the Decree. In general terms, and in very brief summary, the Model is deemed "suitable" where the persons who committed the offence acted deliberately and fraudulently in order to circumvent the safeguards put in place by the Model itself;

- the creation of an internal Supervisory Body, with autonomous powers of initiative and control, tasked with (i) monitoring the effective functioning of the Model and compliance with its provisions by all addressees; (ii) constantly verifying the actual preventive effectiveness of the Model; and (iii) updating it.

In accordance with the provisions of the Decree, with reference to delegated powers and the possible risk of commission of offences, the Model must also:

- identify the activities in the context of which offences may be committed;
- provide for specific controls designed to plan the formation and implementation of the Entity's decisions in relation to the offences to be prevented;
- identify methods of managing financial resources capable of preventing the commission of offences;
- provide for information obligations towards the Supervisory Body;
- introduce a disciplinary system capable of sanctioning failure to comply with the measures set out in the Model.

The adoption of the Model, although not mandatory but merely optional, has exempting effect for the purposes of administrative liability only if accompanied by the effective and concrete implementation of the Model itself and by its constant updating and adaptation.

Indeed, the judge in the criminal proceedings is called upon to assess, within the proceedings aimed at ascertaining the administrative liability of the Entity, the suitability of the Model to prevent the commission of offences, and its actual application and effectiveness.

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

Tagetik Software S.r.l. has its registered, operating and administrative office in LUCCA, Via Roosevelt 103, and its own operating offices/local units in Italy in the cities of Lucca (Via Borgo Giannotti 37/U), Milan (Via Bisceglie 66), Rome (Via Goito 39) and Turin (Wolters Kluwer Italia offices).

Tagetik was founded in 1986 as a consulting firm dealing with Performance Management processes. Although at its inception it was no more than a small company in the Tuscan hills, it rapidly became the fastest-growing "software vendor" of CPM solutions on the market.

In the 1990s Tagetik expanded across Italy and developed its first application suite, consisting of four products for consolidation, budgeting, financial planning, closing and allocations.

In 1994 with Costa Crociere and then in 1997 with Ifil, TAGETIK SOFTWARE S.R.L. began to count among its clients a series of names belonging to the aristocracy of business.

In 2002 UniCredit, the sixth-largest bank in the world, chose Tagetik for statutory consolidation. In this project, Tagetik worked with UniCredit and began the development of Tagetik CPM.

In 2005 Tagetik launched Tagetik CPM (now Tagetik 5), the first fully unified product for all CPM processes, and began expanding its business into other European countries.

In 2008 Tagetik continued its worldwide expansion and opened two offices in North America. Shortly afterwards Gartner placed it in the Visionary Quadrant of its "Magic Quadrant for CPM Suites".

Today Tagetik is a global company offering a unified CPM product, on-premise or in the cloud. With over 50,000 users in 40 different markets, its clients include some of the largest companies in the world listed in the Fortune 1000.

On 6 April 2017 all of the company's shares were acquired by Wolters Kluwer International Holding B.V., which is therefore, as at today's date, the sole shareholder of Tagetik Software S.r.l.

The management of Tagetik Software S.r.l. is currently structured with a Board of Directors composed of 5 Directors, among whom are identified Directors vested with specific powers (to be exercised under sole signature) and members holding the legal representation of the company.

Operationally, the company is organised into 6 Divisions which effectively manage the organisation and day-to-day running of the business, as well as the development of its activities, within the framework of the guidance provided by the Board of Directors.

Among those holding Division roles, certain attorneys-in-fact are also identifiable, in particular for occupational health and safety, the prevention of environmental offences, data protection and compliance with privacy legislation, as well as administrative/financial management.

Since 2012 Tagetik Software has applied the Organisation, Management and Control Model described herein and, as required by Article 6 of Legislative Decree 231/01, has appointed the Supervisory Body tasked with monitoring the effective implementation of the Model itself.

The Organisation, Management and Control Model is integrated with the corporate management systems and, in particular, TAGETIK SOFTWARE S.r.l. has obtained the following certifications from various Bodies:

- UNI EN ISO 9001 – Quality Management System
- ISO 45001 – 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

During 2024 and 2025, all Tagetik Software sites were certified by the third-party body ISOQAR against the UNI EN ISO 14001 reference scheme – Environmental Management System. This management system is integrated with the current quality and safety management systems and ensures over time both the commitment to regulatory compliance and, at the same time, a reduction of the environmental impact of its processes and services with a view to continuous improvement.

This system is also useful in order to mitigate the risk of commission of the environmental offences provided for by Legislative Decree 231/01 under Article 25-*undecies*.

---

3. ORGANISATION AND MANAGEMENT MODEL

3.1 Purpose of the Model

The purpose of the Model is to put in place a structured system of protocols and procedures, together with a series of control and verification activities, capable of preventing, or at least reducing, the risk of commission of the Predicate Offences by the Addressees of the Model.

The Model is intended, among other things, to:

- reaffirm that such forms of unlawful conduct are strongly condemned by TAGETIK SOFTWARE S.R.L., in that they are contrary not only to statutory provisions but also to the ethical and social principles which inspire TAGETIK SOFTWARE S.R.L. in the conduct of its business;

- enable TAGETIK SOFTWARE S.R.L., through an exercise of identification of the areas of activity in which offences may be committed and through the implementation of procedures, to intervene promptly in order to prevent or in any event counter the commission of offences.

It follows that the defining features of the Model are, in addition to the above:

- the awareness-raising and training of all Addressees regarding the rules of conduct and procedures designed to ensure compliance with the Model;
- the mapping of TAGETIK SOFTWARE S.R.L.'s areas of activity in relation to which the Predicate Offences may be committed;
- the conferral upon and attribution to the Supervisory Body of TAGETIK SOFTWARE S.R.L. of specific autonomous powers of initiative and supervision over the effectiveness and proper functioning of the Model;
- the control and documentation of at-risk operations;
- compliance with the principle of segregation of duties;
- the definition of authorisation powers consistent with the responsibilities assigned;
- the verification of the corporate conduct of the Addressees, as well as of the functioning and updating of the Model.

3.2 Structure of the Model

The Model comprises a "General Part" and a number of "Special Parts", drafted in relation to the categories of Offences in respect of which TAGETIK SOFTWARE S.R.L. has considered that a risk of commission exists on the part of the Addressees by virtue of the Business it carries on.

TAGETIK SOFTWARE S.R.L. is aware that the implementation of the Model is, in practice, accompanied by the adoption of a Code of Ethics as well, in which the Entity normally formalises the principles which inspire the conduct of its corporate activity.

It is not TAGETIK SOFTWARE S.R.L.'s intention to depart from that practice, all the more so since the Company has always conducted its business in accordance with a set of principles and rules of conduct inspired by the values of fairness, transparency and good faith.

The original text of the Decree merely identified, as Predicate Offences, certain crimes against the Public Administration and others against property by means of fraud (Articles 24 and 25). Subsequent legislative measures have expanded the number of Predicate Offences for which the administrative liability of the Entity may arise, which has therefore gradually been extended to the following categories:

- computer crimes (Art. 24-*bis*);
- counterfeiting of currency, public credit instruments and revenue stamps (Art. 25-*bis*);
- offences against industry and commerce (Art. 25-*bis*.1);
- corporate offences and private-sector bribery (Art. 25-*ter*);
- offences having the purpose of terrorism or subversion of the democratic order, as well as practices of female genital mutilation (Art. 25-*quater*);
- offences against the individual (Art. 25-*quinquies*);
- offences of insider dealing and market manipulation (Art. 25-*sexies*);
- offences of manslaughter and serious or very serious personal injury committed in breach of occupational health and safety rules (Art. 25-*septies*);
- offences of money laundering, receiving stolen goods and the use of money, goods or benefits of unlawful origin, as well as self-laundering (Art. 25-*octies*);
- offences relating to breach of copyright (Art. 25-*novies*);
- offences against the administration of justice (Art. 25-*decies*);

- environmental offences (Art. 25-*undecies*);
- employment of third-country nationals whose stay is irregular (Art. 25-*duodecies*);
- offences of racism and xenophobia (Art. 25-*terdecies*);
- fraud in sporting competitions, unlawful gaming or betting and gambling by means of prohibited devices (Art. 25-*quaterdecies*);
- tax offences (Art. 25-*quinquiesdecies*);
- smuggling (Art. 25-*sexiesdecies*).

Further extensions of the offences expressly provided for by the Decree are expected in the near future.

For this reason, the Board of Directors of TAGETIK SOFTWARE S.R.L., including at the request of the Supervisory Body, shall adopt appropriate resolutions to supplement the Model with the insertion of new Special Parts relating to those offences which, as a result of further legislative measures, may extend the scope of the Entity's administrative liability.

3.3 General Part

In accordance with Article 6, paragraph 3 of the Decree (and with the aforementioned Guidelines), the General Part of the Model must pursue four fundamental objectives:

I) Identification of the corporate activities in the context of which the Offences may be committed: risk mapping

Article 6, paragraph 2, letter a) of the Decree first requires the Model to carry out the so-called risk mapping: it is therefore necessary to analyse the overall activity carried out by TAGETIK SOFTWARE S.R.L. and to identify the operational or decision-making stages which entail a risk of commission of the Predicate Offences.

Given the legislative measures which have led to a progressive extension of the Predicate Offences, and given also the changes which may occur both in the corporate structure of TAGETIK SOFTWARE S.R.L. and in the activities it carries out, the risk mapping can never be regarded as definitive and unchangeable but must, on the contrary, be subject to ongoing monitoring and review and must likewise be constantly updated.

TAGETIK SOFTWARE S.R.L., with the support of the Supervisory Body, will therefore review and supplement, where necessary, the risk mapping whenever this becomes necessary as a result of further legislative measures, of changes in the corporate structure of TAGETIK SOFTWARE S.R.L., or even merely in consideration of changes in the circumstances and/or in the manner in which TAGETIK SOFTWARE S.R.L. carries on its business.

II) Articulation of a preventive control system

Pursuant to Article 6, paragraph 2, letter b) of the Decree, once the risk mapping has been completed, specific protocols must be provided for in order to plan the formation and implementation of the Entity's decisions in the identified risk areas.

To that end, the individual Special Parts of this Model set out the specific measures defined (including by reference to expressly identified internal procedures) capable of preventing or in any event substantially reducing the risk of commission of the offences.

In addition to those procedures, which have a preventive purpose, the Supervisory Body is expressly granted the power/duty to carry out *ex post* checks on individual transactions or individual corporate conduct.

As with the risk mapping, the procedures and remedies adopted can never be regarded as definitive: on the contrary, their effectiveness and completeness must be the subject of ongoing reassessment by the company and by the Supervisory Body, whose primary task also includes proposing to the Board of Directors such improvements, additions and amendments as it may consider necessary from time to time.

III) Designation of the Supervisory Body

The third objective of the General Part is the identification of a Supervisory Body which, in accordance with the Decree, shall provide for:

- the constant monitoring of compliance with the requirements of the Model, as well as with the specific provisions and procedures put in place to implement it, by all Addressees;
- the constant and continuous assessment of the adequacy of the risk mapping and of the procedures described under points I) and II);
- the proposal to the Board of Directors of all necessary amendments.

The Supervisory Body is a collegial body, internal to TAGETIK SOFTWARE S.R.L., but entirely autonomous and independent, as further specified in section 4 of this Model.

IV) Whistleblowing

The fourth objective of the General Part is to define a system guaranteeing the confidentiality of reports and the protection of whistleblowers. Indeed, by Law No. 179 of 2017 (Official Gazette, General Series No. 291 of 14-12-2017), entitled "Provisions for the protection of persons reporting offences or irregularities of which they have become aware in the context of a public or private employment relationship", the legislator amended Article 6 of Legislative Decree 231/01, providing that the Organisation, Management and Control Model must provide for:

a) one or more channels enabling persons holding functions of representation, administration or management of the entity or of one of its organisational units endowed with financial and functional autonomy, as well as persons who exercise, including on a de facto basis, its management and control, or persons subject to their direction or supervision, to submit, in order to protect the integrity of the entity, detailed reports of unlawful conduct relevant under this decree and founded on precise and consistent factual elements, or of breaches of the entity's organisation and management model, of which they have become aware by reason of the functions performed; such channels must guarantee the confidentiality of the whistleblower's identity in the handling of the report;

b) at least one alternative reporting channel capable of guaranteeing, by electronic means, the confidentiality of the whistleblower's identity;

c) a prohibition on acts of retaliation or discrimination, whether direct or indirect, against the whistleblower for reasons connected, directly or indirectly, with the report;

d) within the disciplinary system adopted pursuant to paragraph 2, letter e), sanctions against those who breach the measures protecting the whistleblower, as well as against those who make, wilfully or through gross negligence, reports which turn out to be unfounded.

It further provided that the adoption of discriminatory measures against persons making the aforementioned reports may be reported to the National Labour Inspectorate, for measures within its competence, not only by the whistleblower but also by the trade union organisation indicated by the latter.

Retaliatory or discriminatory dismissal of the whistleblower is void. Likewise void are the change of duties pursuant to Article 2103 of the Civil Code, as well as any other retaliatory or discriminatory measure adopted against the whistleblower. It is for the employer, in the event of disputes relating to the imposition of disciplinary sanctions, or to demotion, dismissal, transfer, or the subjection of the whistleblower to any other organisational measure having negative effects, whether direct or indirect, on working conditions, subsequent to the submission of the report, to demonstrate that such measures are based on reasons unconnected with the report itself.

Legislative Decree 24/2023 of 10 March 2023, No. 24, "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national regulatory provisions", was recently published in the Official Gazette.

In order to comply with the requirements laid down by the Whistleblowing Decree, the Whistleblowing Directive and Legislative Decree No. 231/2001, this organisational model incorporates the Whistleblowing procedure adopted by Wolters Kluwer Italia S.r.l., as well as the group SpeakUp policy.

The Procedure applies both to the handling of Reports relevant under the Whistleblowing Decree and to the handling of Ordinary Reports, and is based on the following pillars: (i) protection against Reports made in bad faith; (ii) protection of the Whistleblower; (iii) protection of the confidentiality of the Report.

The group policy known as "SpeakUp" is a further tool made available both to all persons forming part of Wolters Kluwer's workforce (employees, contractors, self-employed workers and persons hired through a temporary employment agency, and interns), and to candidates for employment with Wolters Kluwer and former Wolters Kluwer employees, as well as to third parties having a working relationship with Wolters Kluwer, such as shareholders and members of the Wolters Kluwer Supervisory Board, and any person working under the direction of contractors, subcontractors and suppliers providing services to Wolters Kluwer.

This Policy describes when, where and how to report any concerns regarding alleged misconduct or a breach of the corporate Code of Ethics, of other corporate policies or of the law.

The persons involved in this Procedure act in compliance with the regulatory and organisational system, with internal powers and delegations, and are required to act in accordance with applicable laws and regulations as well as corporate policies, and in compliance with the principles set out below:

KNOWLEDGE AND AWARENESS – The Procedure is a fundamental element in ensuring full awareness for the effective oversight of risks and their interrelations and in guiding changes in strategy and in the organisational context.

PROTECTION OF THE REPORTED PERSON AGAINST REPORTS MADE IN "BAD FAITH" – All persons are required to respect the dignity, honour and reputation of others. To that end, the Whistleblower is required to declare whether they have a private interest connected with the Report. More generally, the Company guarantees adequate protection against Reports made in "bad faith", censuring such conduct and making it known that Reports submitted for the purpose of causing damage or otherwise prejudice, as well as any other form of abuse of this document, give rise to liability, in disciplinary proceedings and in other competent fora. In the context of Reports relevant under the Whistleblowing Decree, Reported Persons enjoy the protections provided for by the Whistleblowing Decree.

IMPARTIALITY, AUTONOMY AND INDEPENDENCE OF JUDGEMENT – All persons who receive, examine and assess Reports possess the requisite moral and professional standing and ensure that the necessary conditions of independence and due objectivity, competence and diligence are maintained in the performance of their activities.

The Supervisory Body is kept constantly informed regarding the handling of Reports on the basis of the provisions of paragraph 8 of the aforementioned Whistleblowing procedure. The Supervisory Body is a recipient of the Half-Yearly Reports Report and of the periodic reports (at least on an annual basis) referred to in paragraph 10 of the aforementioned Whistleblowing procedure. The Supervisory Body handles Reports pursuant to paragraph 8 of the aforementioned Whistleblowing procedure where there are conflicts of interest on the part of the Whistleblowing Committee. Once it has received the final written report on the Report, the Supervisory Body may decide to carry out further independent investigations and assessments, including by using its own budget.

3.4 Special Parts

In addition to the General Part described above, this Model comprises a number of Special Parts, each dedicated to a specific category of Predicate Offences in respect of which, on the basis of the risk mapping carried out pursuant to the Decree, TAGETIK SOFTWARE S.R.L. has considered that a risk of commission exists within the organisation.

Each Special Part, in addition to describing the criminal offences examined, identifies the corporate areas considered to be particularly at risk, as well as setting out precisely the procedures adopted in order to avoid or at least reduce the commission of the unlawful acts.

The Special Parts which follow therefore examine the following categories:

i) Offences against the Public Administration (Special Part "A");
ii) Computer crimes and unlawful data processing, as well as copyright offences (Special Part "B");
iii) So-called corporate offences and private-sector bribery (Special Part "C");
iv) Market abuse (Special Part "D");

v) Manslaughter and serious or very serious negligent personal injury, committed in breach of accident-prevention rules and rules on occupational hygiene and health (Special Part "E");
vi) Offences of money laundering, receiving stolen goods and the use of money, goods or benefits of unlawful origin, as well as self-laundering (Special Part "F");
vii) Employment of third-country nationals whose stay is irregular (Special Part "G");
viii) Tax offences (Special Part "H").

Following the risk mapping initially carried out in 2012, then updated in 2017 and, finally, in the present year 2020, TAGETIK SOFTWARE S.R.L. has considered it appropriate not to include in this Model the offences having the purpose of terrorism or subversion of the democratic order, as well as those of organised crime, or the offences against industry and commerce, environmental offences, sporting fraud, unlawful gambling and smuggling offences – for which the administrative liability of the Entity is nonetheless provided – in consideration of the fact that there are no real and concrete/significant risks of commission of such offences, having regard to the specific corporate activities carried out by the Company.

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

In the light of its intention to operate in a transparent and proper manner, also in order to safeguard its corporate reputation as well as that of its shareholders, directors and employees, TAGETIK SOFTWARE S.R.L. has considered it appropriate, and in line with its corporate philosophy, to proceed with the adoption and implementation of this Model, and with its subsequent constant updating.

The Model is also intended to raise the awareness of all Addressees, so as to guide their conduct according to principles of fairness and transparency and, at the same time, to avoid and prevent any risk of commission of offences in the course of corporate activities.

The Model has been prepared by TAGETIK SOFTWARE S.R.L. having regard to its own specific organisation, size and structure, to the requirements and rules of the Decree, to the relevant case law, as well as to the Guidelines drawn up by trade associations and, in particular, those drawn up by Confindustria (in the version published on the Confindustria website in March 2014).

This Model was adopted by the Board of Directors of Tagetik Software S.r.l. by specific resolution. The Board of Directors has also appointed the Supervisory Body, currently composed of 2 members and endowed with autonomous powers, with tasks of supervision, control and initiative in relation to the Model itself and, in particular, to its actual application, observance and updating.

3.6 Risk mapping

On the basis of the provisions of the Decree and of the indications provided by the Guidelines, TAGETIK SOFTWARE S.R.L. has carried out the risk mapping, identifying, within its corporate reality, the areas which are particularly at risk of commission of any of the Predicate Offences.

The methodology used for the risk mapping is briefly illustrated below.

TAGETIK SOFTWARE S.R.L. first analysed the constituent elements of the Predicate Offences, in order to identify and define the specific conduct which, within its corporate activities, could give rise to the various criminal offences.

Secondly, TAGETIK SOFTWARE S.R.L. analysed its corporate reality in order to identify the areas and sectors most at risk. The identification of such risk areas was initially carried out with the support of a lawyer and of an external consultant specialising in business organisation, specifically appointed for that purpose, analysing the reality of TAGETIK SOFTWARE S.R.L. on the basis of interviews with the Directors and Process Owners and of the analysis of a sample of the documents used for the management of corporate activities. The updating of the risk mapping was carried out in 2016 with the operational support of the Supervisory Body.

Finally, TAGETIK SOFTWARE S.R.L. proceeded to draft, within the risk areas identified during the initial assessment, the procedures and protocols considered appropriate in order to ensure the adequacy and efficiency of the model in relation to the provisions of the Decree. The outcomes of the aforementioned risk-mapping activities are described in detail in the individual Special Parts, where the procedures and measures put in place by TAGETIK SOFTWARE S.R.L. in order to avoid or in any event minimise the risk of commission of the Predicate Offences are also illustrated.

3.7 Addressees of the Model

The addressees of the rules and requirements contained in this Model, and therefore bound to comply with it in full, are, in general, all those who act in the name and on behalf of TAGETIK SOFTWARE S.R.L., including directors, the members of any other corporate bodies, employees, collaborators (including occasional ones), business partners, suppliers, and the members of the Supervisory Body.

---

4. SUPERVISORY BODY

4.1 Identification of the Supervisory Body

The Supervisory Body of TAGETIK SOFTWARE S.R.L. is an internal body endowed with autonomous powers of initiative and control, tasked with supervising the functioning of and compliance with the Model and with providing for its updating.

The Supervisory Body of TAGETIK SOFTWARE S.R.L. is composed of two members, to be selected from among persons of proven competence and professionalism, who, at their first meeting, shall adopt specific rules governing its functioning.

In the light of the experience gained in practice, and in compliance with the provisions of the Decree, TAGETIK SOFTWARE S.R.L. has considered it appropriate to identify, as members of its Supervisory Body, two external professionals with expertise in the subject matter of the Decree, namely a chartered accountant with long-standing knowledge of the company and an engineer specialising in management systems and business organisation with long-standing knowledge of the company.

This solution is considered by TAGETIK SOFTWARE S.R.L. to be the optimal choice, as it enables the Supervisory Body to operate effectively across the various corporate areas with full knowledge of the activities concerned.

The Supervisory Body is appointed by the Board of Directors of TAGETIK SOFTWARE S.R.L. and remains in office for the term indicated in the instrument of appointment or, failing such a term, for three years. Its members may hold office for more than one term, with no limit on the number of terms.

The following constitute grounds of ineligibility for, or removal from, membership of the Supervisory Body:

i) conviction, including by a non-final judgment or by plea bargaining, for intentional offences — thus excluding negligent offences, save for those provided for and punished by Articles 589 and 590, paragraph 3 of the Criminal Code, committed in breach of accident-prevention rules and rules on occupational hygiene and health — as well as for contraventions entailing the application of an ancillary penalty under Article 19 of the Criminal Code, or provided for by specific statutory provisions;

ii) in any event, any conviction, including non-final, entailing the application of an ancillary penalty under Article 19 of the Criminal Code or provided for by specific statutory provisions;

iii) the application of a security measure, whether personal or in rem, the application of a preventive measure, whether personal or in rem, or the application of an anti-mafia preventive measure, whether personal or in rem;

iv) a declaration of legal incapacity or disability under the Civil Code, as well as a conflict of interest with TAGETIK SOFTWARE S.R.L.

Grounds for suspension from office, for the entire duration of the measure, are also constituted by the application of a personal precautionary measure (pre-trial detention in prison or in a care facility, house arrest, prohibition or obligation of residence, obligation to report to the Judicial Police, prohibition on leaving the country) and the application of a disqualifying measure (suspension from the exercise of a public office or service, temporary prohibition on carrying out certain professional and entrepreneurial activities).

The Civil Code rules on mandate shall apply to the Supervisory Body and its members.

4.2 Prerogatives and resources of the Supervisory Body

The Supervisory Body may avail itself of the cooperation of persons belonging to the various corporate functions, where their specific knowledge and expertise are required for particular analyses, and for the assessment of specific operational and decision-making steps in TAGETIK SOFTWARE S.R.L.'s activities.

In any event, the Supervisory Body shall have the option, where the need arises to make use of professional expertise not available internally, or in any event within the organisation chart of TAGETIK SOFTWARE S.R.L., to use the services of external professionals.

At the beginning of its term of office, and thereafter on an annual basis, the Supervisory Body may submit to the Board of Directors of TAGETIK SOFTWARE S.R.L. a request for an annual expenditure budget to be provided by TAGETIK SOFTWARE S.R.L. itself and, in particular:

- the Supervisory Body shall submit to the Board of Directors a request for the availability of the amount corresponding to the annual budget, with sufficient detail of the expenses and costs to be incurred for the proper performance of its mandate;
- the Board of Directors may not reasonably refuse to make that amount available, it being understood that the Supervisory Body may use it autonomously and without any obligation of prior authorisation, for the purposes provided for by this Model;
- that amount must cover the expenses which, according to estimates, the Supervisory Body will have to incur in the exercise of its functions (it being understood that any costs relating to human or material resources made available by TAGETIK SOFTWARE S.R.L. do not form part of the budget).

Should, by reason of extraordinary events or circumstances (that is, outside the ordinary conduct of the Supervisory Body's activities), the Supervisory Body require the availability of amounts in addition to the amount indicated above, the Chair of the Supervisory Body shall submit a reasoned request to the Board of Directors of TAGETIK SOFTWARE S.R.L., setting out in reasonable detail the reasons and facts underlying that request. The request for additional funds may not be rejected by the Board of Directors without well-founded reason.

4.3 Functions and powers of the Supervisory Body

The Supervisory Body of TAGETIK SOFTWARE S.R.L. is entrusted with the task of:

- supervising compliance by the Addressees with the requirements of the Model and of the documents connected with it, taking all necessary initiatives;
- supervising the actual effectiveness, efficiency and real capacity of the requirements of the Model, in relation to the corporate structure, to prevent the commission of the Predicate Offences;
- verifying the appropriateness of updating and adapting the procedures governed by the Model, submitting the relevant proposals to the Board of Directors;
- reporting to the Board of Directors any ascertained breaches of the Model so that it may take the consequent measures.

Without prejudice to the duty of supervision over compliance with the Model and with the procedures set out therein, which is attributed to the Supervisory Body, its actions are not subject to review by the Board of Directors, except on grounds relating to non-performance of the mandate conferred.

In particular, the Supervisory Body of TAGETIK SOFTWARE S.R.L. shall pursue the aforementioned objectives through:

- surveys of corporate activities, for the purposes of the periodic verification of the implementation of the provisions of the Model as well as for updating the mapping of risk areas within the corporate context;

- requests for periodic or specific information from individual corporate functions in relation to activities considered to be at risk. The information requested by the Supervisory Body must be promptly provided by the functions concerned without any omission or alteration whatsoever, in order to ensure that the Body has a certain and concrete view of the activities under monitoring; to that end, it is also specified that the Supervisory Body must be kept constantly informed of developments in the risk areas, and has free access to all the relevant corporate documentation;

- coordination with the other corporate functions (including through specific meetings) for the better monitoring of activities in the areas identified as being at risk of commission of the predicate offences;

- coordination with the heads of the corporate functions on the various aspects relating to the implementation of the Model;

- verification of the actual existence and proper maintenance of the documentation required in accordance with the provisions of the individual Special Parts of the Model for the various categories of offence;

- any other control, whether periodic or targeted, of the actual conduct of individual operations, procedures or activities within TAGETIK SOFTWARE S.R.L. which may be appropriate.

In addition, the Supervisory Body shall:

- verify the adequacy of the rules in force in relation to any transformations, changes and expansions of the corporate business;
- report to the Board of Directors any shortcomings in the Model and the related proposals for amendment or improvement;
- consequently see to the updating of the rules of conduct of the individual Special Parts;
- verify the validity of the standard clauses aimed at implementing sanctioning mechanisms (for example, those providing for termination of contracts with business partners, collaborators or suppliers) where breaches of the requirements of the Decree are ascertained.

The Supervisory Body shall prepare an information report addressed to the Board of Directors, at least on an annual basis.

Finally, and in accordance with the provisions of Article 6, paragraph 1, letter b) of the Decree, the monitoring and updating tasks assigned to the Supervisory Body in respect of the Model are articulated into three different types of verification:

- **verifications of acts:** periodically, the Supervisory Body shall carry out a review of the principal corporate acts and of any contracts of significant importance entered into by TAGETIK SOFTWARE S.R.L. within the risk areas;

- **verifications of procedures:** periodically, the Supervisory Body shall verify the actual implementation of this Model;

- **verifications of reports and measures:** the Supervisory Body shall examine every report received during the year, the actions taken in that regard, the events and episodes considered most at risk, as well as the effectiveness of the knowledge among all Addressees of the content of the Model and of the categories of offence for which the administrative liability of the entity is provided.

The Supervisory Body must account for the results of this verification activity, albeit in summary form, in the report prepared annually by the Supervisory Body for the Board of Directors, the Board of Statutory Auditors and 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. may be contacted in 3 ways:

- personal contact with one of the members and the possible joint drafting of a document addressed to the Supervisory Body;
- e-mail communication to the mailbox organismodivigilanza@tagetik.com;
- written reports, including anonymous ones, sent in a sealed envelope to the address: Organismo di Vigilanza c/o Tagetik Software S.r.l., Via Roosevelt 103, 55100 LUCCA.

The Supervisory Body is required to conduct internal investigations following reports of possible breaches of this Model and, where these are considered serious and well-founded, to formulate non-binding opinions on the type and extent of the measures to be adopted as well as on the possible sanctions to be imposed on those responsible. The implementation of the measures and of any sanctions is a matter for the Board of Directors, which determines their extent taking into account the opinions and indications of the Supervisory Body. The Supervisory Body is required to guarantee whistleblowers acting in good faith against any form of retaliation, discrimination or penalisation.

5.2 Information obligations towards the Supervisory Body

In addition to the documentation expressly indicated by each individual Special Part of the Model in accordance with the procedures contemplated therein, the Supervisory Body must be informed of any other information relating to the implementation of the Model in the risk areas, as well as information relating to any breaches of the requirements of the Model itself.

The following information must always be communicated to the Supervisory Body:

- decisions relating to the request for, granting and use of public financing;
- requests for legal assistance submitted by employees (including managers) against whom the judicial authorities are proceeding in respect of any of the Predicate Offences;
- measures and/or information originating from the Judiciary and from Judicial Police bodies or from any other authority, from which it appears that investigations are being

conducted, including against persons unknown, for facts potentially involving the corporate activities of TAGETIK SOFTWARE S.R.L.;

- the results and conclusions of commissions of inquiry or other internal reports from which hypotheses of liability for the Predicate Offences emerge;
- information relating to the actual implementation of the Model at all corporate levels;
- disciplinary proceedings conducted, any sanctions imposed or decisions to close such proceedings, together with the relevant reasons;
- summary statements of contracts awarded following public tenders or private negotiations;
- orders awarded by public bodies, by the European Community or by persons performing functions of public utility;
- accidents and incidents at work classifiable as serious or very serious (indicatively, with an initial prognosis of more than 40 days).

The Board of Directors is required to provide the Supervisory Body with full information on matters falling within the competence of the Supervisory Body itself.

In order to enable the Supervisory Body to perform effectively the tasks entrusted to it, TAGETIK SOFTWARE S.R.L. guarantees to all Addressees of the Model, as well as to any third parties, the right to report to that body any unlawful act, anomaly or suspicious activity in relation to the commission of, or the risk of commission of, one of the Predicate Offences, of which they have become aware for any reason whatsoever.

To all those who send communications or reports to the Supervisory Body, TAGETIK SOFTWARE S.R.L. expressly guarantees the exclusion of any form of retaliation, discrimination or penalisation and, in any event, ensures the confidentiality of the whistleblower's identity.

All employees of the company therefore have the right, as well as the duty, to communicate in writing any information relating to possible internal anomalies or unlawful activities.

The Supervisory Body may also receive and assess reports and communications, likewise in writing, from persons outside the company.

The Supervisory Body may request any kind of information and/or documentation useful for the investigations and controls entrusted to it from the Board of Directors and from employees, who are obliged to comply with the utmost care, completeness and promptness with every request of the Supervisory Body.

The Supervisory Body of TAGETIK SOFTWARE S.R.L. must receive detailed information from the Board of Directors regarding any changes to the powers defined and to the delegations conferred.

The Supervisory Body verifies and analyses the information and communications received and the measures to be implemented; once implemented, the measures must be in line with and comply with the provisions laid down by the disciplinary system of this Model.

The Supervisory Body may request the Board of Directors to impose disciplinary sanctions on those who fail to comply with the information obligations.

The Supervisory Body shall inform the Board of Directors, for its own determinations, if, following the investigations carried out into the communications and reports received, these

were drawn up wilfully or through gross negligence with the aim of damaging the company, its directors, managers and employees.

5.3 Information obligations of the Supervisory Body towards the corporate bodies

The Supervisory Body is subject to specific information obligations towards the Board of Directors and the Shareholders' Meeting.

The Supervisory Body shall also have the specific obligation to provide prompt information on any amendment, addition or update which may affect the Decree. The Supervisory Body also has the duty to communicate to the Board of Directors any breach ascertained in the course of carrying out its activities.

The Supervisory Body of TAGETIK SOFTWARE S.R.L. may be convened at any time by the Board of Directors or may in turn request to be heard by the latter, in order to report on the functioning of the Model or on specific situations.

In addition, on an annual basis, as already defined above, the Supervisory Body submits to the Board of Directors (and to the Shareholders' Meeting) a written report on the implementation of the Model.

5.4 Collection and retention of information

The information and reports prepared or received pursuant to the Decree must be retained by the Supervisory Body in a dedicated archive, whether electronic or paper-based, which, subject to the written authorisation of the Supervisory Body itself, may be made accessible to external parties in accordance with procedures to be defined by the Supervisory Body.

That documentation will of course be available to the Supervisory Body and to anyone having an interest in consulting it.

By its own choice, the Supervisory Body has decided to use a minute book with certified pages.

---

6. DISCIPLINARY SYSTEM

6.1 General principles

Article 6, paragraph 2, letter e) of the Decree provides that a disciplinary system capable of sanctioning any breaches must be introduced.

The definition of a disciplinary system (to be proportionate to the type of infringement) to be applied in the event of breach of the provisions of the Model gives effect to the supervisory and preventive action entrusted to the Supervisory Body and is intended to ensure the effectiveness of the Model itself.

The disciplinary system has also been drafted on the basis of the following principles:

- differentiation according to the Addressees of the Model;

- identification of the disciplinary sanctions to be adopted in respect of the addressees in compliance with the provisions of the applicable national collective bargaining agreements (CCNL) and applicable statutory requirements;
- identification of procedures for ascertaining breaches, infringements, circumventions, imperfect or partial application, as well as of a specific procedure for imposing the applicable sanctions, identifying the person responsible for imposing them and, more generally, for supervising the observance, application and updating of the disciplinary system.

In particular, the disciplinary system is addressed to:

- all those who hold, including on a de facto basis, functions of representation, administration or management (including any liquidators) of TAGETIK SOFTWARE S.R.L. or of one of its organisational units endowed with financial and managerial autonomy;

- persons subject to the direction or supervision of one of the aforementioned persons, and more generally all employees as well as all those who, on any basis and at various levels of responsibility, operate within TAGETIK SOFTWARE S.R.L., contributing through their acts to the conduct of the overall corporate activity, including collaborators, business partners and suppliers.

This disciplinary system is divided into specific sections, each relating to a category of addressees, taking into account the legal status of the various persons concerned.

The Supervisory Body is entrusted with the task of supervising the observance and proper application of the disciplinary system and its effectiveness, as well as of adopting appropriate measures so that the Board of Directors of TAGETIK SOFTWARE S.R.L. updates, amends and/or supplements the disciplinary system itself.

The application of disciplinary sanctions is independent of the outcome of any criminal proceedings, since the rules of conduct imposed by the Model are assumed by the company in full autonomy, irrespective of the criminal offence which such conduct may constitute.

The Supervisory Body may propose to the Board of Directors of TAGETIK SOFTWARE S.R.L. the adoption of disciplinary measures proportionate to the extent and gravity of the breaches ascertained.

6.2 Disciplinary sanctions against employees

Conduct by employees in breach of the individual rules of conduct set out in this Model shall constitute disciplinary offences.

The sanctions which may be imposed on employees are among those provided for by the collective bargaining agreement applied within the company, in compliance with the procedures laid down by Article 7 of Law No. 300 of 30 May 1970 (the so-called Workers' Statute) and any applicable special legislation.

In particular, the sanctions imposed may, depending on the gravity of the breach, be those provided for by the Commerce CCNL, as well as by the CCNL for Commerce Executives.

Sanctions shall be imposed, in compliance with the procedures laid down by the applicable CCNL, by the Board of Directors, on its own initiative or at the proposal of the Supervisory Body.

In matters of occupational health and safety, the application of disciplinary sanctions may be proposed by the Head of the Prevention and Protection Service (RSPP) and/or by the Employer.

The disciplinary measures listed below, which may be imposed on non-executive staff, are those provided for by the sanctioning framework of the CCNL and any amendments and renewals of that agreement, and shall be adopted taking into account:

- the intentionality of the conduct and the degree of negligence, imprudence or lack of skill, having regard also to the foreseeability of the event;
- the overall conduct of the worker, with particular regard to the existence or otherwise of prior disciplinary records within the limits permitted by law;
- the duties of the worker;
- the functional position of the persons involved in the facts constituting the misconduct;
- any other particular circumstances accompanying the disciplinary breach.

All the provisions of Article 7 of Law 300/1970 remain in force and are hereby recalled, both as regards the display of disciplinary codes and, in particular, the obligation to notify the employee in advance of the charge, also in order to enable the latter to prepare an appropriate defence and to provide any justifications, as well as for the purposes of the relevance of recidivism.

Accordingly, the disciplinary measures which may be imposed on such workers, in compliance with the provisions laid down by Article 7 of the Workers' Statute (Law No. 300 of 20 May 1970) and any applicable special legislation, are those provided for by the sanctioning framework of the CCNL for the commerce sector, and specifically:

1. **Verbal reprimand:** applies in the event of minor non-compliance with the principles and rules of conduct laid down by the Organisational Model and/or the Code of Ethics, or in breach of internal procedures or rules.

2. **Written reprimand:** applies in cases of repetition of the infringements referred to in point 1 above.

3. **Fine not exceeding 4 hours of normal pay:** applies in the event of non-compliance with the principles and rules of conduct laid down by the Organisational Model and/or the Code of Ethics or in the event of breach of internal procedures and rules, to an extent such that it may be considered, although not minor, nonetheless not serious, such conduct being linked to negligent non-compliance with the rules and/or procedures and/or with the directives and instructions issued by management or by superiors.

4. **Suspension from pay and from duty for a maximum of 10 days:** applies in the event of non-compliance with the principles and rules of conduct laid down by the Organisational Model and/or the Code of Ethics or in the event of breach of internal procedures and rules, to an extent such as to be considered of a certain gravity, including where it results from repetition of any disciplinary offence sanctioned by a fine.

5. **Disciplinary dismissal without notice and subject to the other conditions of reason and law:** applies in the event of the adoption, in carrying out the activities included within

the Sensitive Activities, of conduct characterised by significant non-compliance with the requirements and/or procedures and/or internal rules laid down by the Organisational Model and/or the Code of Ethics, even if such conduct is merely capable of constituting one of the offences or administrative violations sanctioned by the Decree, or in the event of repetition of any disciplinary offence sanctioned by suspension.

In the event of non-compliance by executives with the principles and rules of conduct laid down by the Organisational Model and the Code of Ethics, or in the event of breach of the internal procedures and rules provided for and/or referred to, or further in the event of the adoption, within the scope of Sensitive Activities, of conduct which is not compliant with or not adequate to the aforementioned requirements, the most appropriate measures shall be applied to those responsible in accordance with the provisions of the National Collective Bargaining Agreement for Commerce Executives. It also constitutes an offence for executive staff to fail to supervise the proper application, by hierarchically subordinate workers, of the rules and procedures laid down by the Organisational Model and the Code of Ethics, as well as the direct breach thereof, or more generally the adoption of conduct, in carrying out the activities connected with their duties, which is not in line with the conduct reasonably expected of an executive, having regard to the role held and the degree of autonomy granted.

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 binding on all addressees. Accordingly, those documents and any subsequent updates thereof are brought to the attention of the addressees by the Company through the circulation of an internal memorandum in accordance with the provisions of Article 7 of the Workers' Statute, giving particular prominence to the sanctions connected with breaches.

6.3 Measures against directors and statutory auditors

In the event of breaches of the Model by the directors of TAGETIK SOFTWARE S.R.L., the Supervisory Body shall inform the entire Board of Directors and, if considered appropriate, the Shareholders' Meeting, which shall take the appropriate initiatives provided for by the legislation in force.

6.4 Measures against collaborators, business partners and suppliers

Any conduct by collaborators, business partners or suppliers which is contrary to the lines of conduct set out in this Model and such as to entail the risk of commission of a Predicate Offence may result, in accordance with the specific contractual clauses included in the engagement letters or partnership agreements, in the termination of the contractual relationship, without prejudice to a claim for damages where such conduct causes damage to TAGETIK SOFTWARE S.R.L., as in the case of the application by the Court of the measures provided for by the Decree.

---

7. DISSEMINATION AND KNOWLEDGE OF THE MODEL

A prerequisite for the Model to constitute an exemption from the administrative liability of the Entity is its effectiveness, as well as its concrete and effective application.

An essential condition for ensuring the concrete and constant observance of the Model and of the procedures described therein is knowledge of the Model by all Addressees.

TAGETIK SOFTWARE S.R.L. has therefore adopted the initiatives described below in order to ensure the proper dissemination of the Model not only within but also outside its corporate organisation.

7.1 Staff training

TAGETIK SOFTWARE S.R.L. promotes knowledge of the Model among all Addressees, who are therefore required to know its content, to observe it and to contribute to its better implementation.

For the purposes of implementing the Model, staff training (to which external consultants must also be added) shall be structured as follows:

- initial training through specific meetings in the period immediately following the approval of the Model and of any subsequent substantive revision;
- circulation of an internal information note explaining the Model and its functions;
- publication on the website and intranet of TAGETIK SOFTWARE S.R.L. of this Model and of the Code of Ethics connected with it;
- publication on the intranet of TAGETIK SOFTWARE S.R.L. of the internal procedures connected with this Model;
- circulation, by internal memorandum, of information material dedicated to the subject, with constant and prompt communication of any updates and amendments;
- information provided at the time of recruitment.

7.2 Information for collaborators, business partners and suppliers

TAGETIK SOFTWARE S.R.L. promotes knowledge of and compliance with the Model also among business partners, collaborators and suppliers, through the publication of this Model on the corporate website.

7.3 Contractual clauses

In order to ensure compliance with the requirements and procedures set out in this Model also by third parties who participate, including indirectly, in the conduct of TAGETIK SOFTWARE S.R.L.'s business, the Company shall include in contracts and engagement letters signed with business partners, suppliers and collaborators specific contractual clauses whereby the signatories undertake to comply with the rules of the Model, also accepting that any breach thereof may constitute grounds for termination of the relevant contract by TAGETIK SOFTWARE S.R.L.

The Company indeed considers that this contractual remedy constitutes the only instrument enabling it to protect compliance with the procedures and principles developed by the Model also on the part of persons (such as collaborators and business partners) who are not exposed to the risk of the disciplinary sanctions expressly provided for employees.

SPECIAL PART "A" — Relations with the Public Administration

1. The categories of offence in dealings with the Public Administration (Articles 24 and 25 of the Decree)

As regards this First Special Part, a brief description is given below of the offences contemplated therein, set out in Articles 24 and 25 of the Decree:

Misappropriation to the detriment of the State or the European Union (Art. 316-*bis* of the Criminal Code) This offence arises where, after receiving financing or contributions from the Italian State or from the European Union, the sums obtained are not used for the purposes for which they were intended (the conduct consists in having diverted, even partially, the sum obtained, irrespective of whether the planned activity was nonetheless carried out). Given that the moment of completion of the offence coincides with the implementation stage, the offence may also arise with reference to financing already obtained in the past and subsequently not allocated to the purposes for which it was granted.

Undue receipt of disbursements to the detriment of the State or the European Union (Art. 316-*ter* of the Criminal Code) This offence arises where — through the use or presentation of false declarations or documents, or through the omission of required information — contributions, financing, subsidised loans or other disbursements of the same kind granted or paid by the State, by other public bodies or by the European Union are obtained without entitlement. In this case, unlike the preceding point (Art. 316-*bis*), the use made of the disbursements is irrelevant, since the offence is completed at the moment the financing is obtained. Finally, it should be noted that this offence is residual in relation to the offence of fraud against the State (described below), in the sense that it arises only in cases where the conduct does not amount to fraud against the State.

Extortion by a public official (Art. 317 of the Criminal Code) This offence arises where a public official or a person entrusted with a public service, abusing their position, compels another person to give or promise to them or to third parties money or other benefits not due. This offence is capable of merely residual application within the categories considered by the Decree; in particular, within the scope of application of the Decree, this form of offence could arise where an employee or agent of a company is an accomplice to the offence of the public official who, taking advantage of that capacity, requests undue services from third parties (provided that such conduct results in some way in an advantage for the company).

Bribery for an act of office or an act contrary to the duties of office (Arts. 318–319 of the Criminal Code) This offence arises where a public official receives, for themselves or for others, money or other advantages in order to perform, omit or delay acts of their office (thereby creating an advantage in favour of the offeror). The public official's activity may consist either in an act which is due (for example: expediting a matter falling within their competence) or in an act contrary to their duties (for example: a public official who accepts money to secure the award of a tender). This offence differs from extortion by a public official in that, between the bribed person and the briber, there is an agreement aimed at achieving a mutual advantage, whereas in extortion the private party is subject to the conduct of the public official or of the person entrusted with a public service.

Incitement to bribery (Art. 322 of the Criminal Code) This offence arises where, in the presence of conduct aimed at bribery, the public official refuses the unlawful offer made to them.

Bribery in judicial acts (Art. 319-*ter*) This offence arises where the Company is a party to judicial proceedings and, in order to obtain an advantage in those proceedings, bribes a public official (not only a judge, but also a clerk, a witness or another official).

Fraud to the detriment of the State, another Public Body or the European Union (Art. 640, paragraph 2, no. 1, of the Criminal Code) This offence arises where, in order to obtain an unjust profit, artifices or deceptions are employed such as to mislead and cause damage to the State (or to another Public Body or to the European Union), inducing it to provide a given financial benefit. This offence may arise, for example, where, in preparing documents or data for participation in tender procedures, untruthful information is provided to the Public Administration (for example, supported by falsified documentation) in order to secure the award of the tender.

Aggravated fraud to obtain public disbursements (Art. 640-*bis* of the Criminal Code) This offence arises where the fraud is committed in order to obtain public disbursements unduly. This offence may arise where artifices or deceptions are employed, for example by communicating untrue data or preparing false documentation, in order to obtain public financing.

Computer fraud to the detriment of the State or another Public Body (Art. 640-*ter* of the Criminal Code) This offence arises where, by altering the operation of a computer or telematic system or by manipulating the data contained therein, an unjust profit is obtained from the State or another public body, causing damage to third parties. In practice, the offence in question could arise where, once financing has been obtained, the computer system is breached in order to enter an amount of financing higher than that legitimately obtained.

Fraud in public supplies (Art. 356 of the Criminal Code) The offence arises where fraud is carried out in the course of the provision of a supply (whether of products and/or services) to the State, to a local authority or in any event to a body of the Public Administration, including companies with a majority public shareholding. The offence presupposes the existence of a contract under which supplies different from those agreed are provided. As it involves general intent, neither deception nor defects in the goods supplied are required; bad faith in the performance of the contract is sufficient.

Fraud to the detriment of the European Agricultural Fund (Art. 2, Law No. 898 of 23/12/1986) The offence arises where any person, by presenting false data or information, unduly obtains, for themselves or for others, aid, premiums, allowances, refunds, contributions or other disbursements charged in whole or in part to the European Agricultural Guarantee Fund and the European Agricultural Fund for Rural Development.

Embezzlement (Art. 314 of the Criminal Code) The offence arises where a public official or a person entrusted with a public service misappropriates money or other property belonging to others of which they are in possession or which is at their disposal by reason of their office or service.

Embezzlement by taking advantage of another's error (Art. 316 of the Criminal Code) The offence arises where a public official or a person entrusted with a public service, in the exercise

of their functions, receives or retains money or obtains other benefits, taking advantage of another's error, to the benefit of themselves or of third parties.

Abuse of office (Art. 323 of the Criminal Code) This offence is committed by a public official or a person entrusted with a public service who, in the performance of their functions, procures for themselves or for others an undue financial advantage or causes unjust damage to others, in breach of statutory rules or of the entity's regulations, or by failing to abstain in the presence of their own interest or that of a close relative.

2. Assessment of the Risk Areas

Irrespective of the fact that the risk of commission of offences against the Public Administration is present in every business activity (any company will, in the course of its ordinary activities, deal on more than one occasion with different public bodies and for different reasons, first and foremost the incorporation of the company, with reference to the formal registration and publication requirements), the risk of unlawful acts in dealings with the Public Administration has been considered not negligible in TAGETIK SOFTWARE S.R.L. by reason of the fact that, although TAGETIK SOFTWARE S.R.L.'s clientele consists mainly of private companies, in some cases the recipients of TAGETIK SOFTWARE S.R.L.'s services are public companies and/or companies with a majority public shareholding (e.g. so-called municipal utilities). Following that assessment, the ethical principles governing the management of relations with the public administration have been included in the corporate code of ethics and specific procedures have been provided for the reduction and control of the risk of unlawful acts.

3. Identification of the At-Risk Activities

The offences considered presuppose, as stated, the establishment of relations with the Public Administration (understood in a broad sense so as to include also the Public Administration of foreign States, as well as representatives of private bodies or private parties which nonetheless carry out activities governed by rules of public law and, in general, of public interest).

All corporate activities which involve the establishment of a relationship with the Public Administration are therefore to be regarded as at risk (direct risk activities).

Equally to be regarded as at risk are those corporate areas which, although not directly involving the establishment of relations with the Public Administration, manage financial and payment instruments and other activities which could enable advantages and benefits to be conferred on public officials (or on persons connected with them) in the commission of offences against the Public Administration (indirect risk activities).

Indirect risk areas include, in particular (with reference to the possibility that they may be used to create hidden reserves of money to be used, as the case may be, for unlawful payments, or to conceal such unlawful payments):

- administration, finance, accounting and tax activities;
- payment activities, with reference to the possibility that the parties selected may be connected with local administrators and public officials, such that the award of the engagement may be the consideration for a corrupt agreement or in any event for an unlawful advantage;

- the award of consultancy and professional service contracts, in particular where the party selected operates in contact with the public administrative area to which TAGETIK SOFTWARE S.R.L. is addressing itself at that time;
- staff selection;
- the appointment of executives and members of corporate bodies.

4. Principles of conduct in the management of direct-risk activities

This Special Part provides for an express prohibition — binding on all Addressees — on:

I) engaging in conduct such as to constitute the categories of offence considered above (Articles 24 and 25 of the Decree);
II) engaging in conduct which, although not in itself constituting the categories of offence considered above, could potentially become such or in any event present itself in an unclear manner and be open to misunderstanding;
III) creating any situation of conflict of interest in dealings with the Public Administration in relation to the aforementioned categories of offence.

In the context of any relationship with the Public Administration, it is in particular prohibited to:

a) make cash payments to public officials;

b) distribute gifts and presents to Italian and foreign public officials (including in those countries where the giving of gifts is a widespread practice), or to their family members, which may influence their independence of judgement or induce them to secure any advantage for the Company. Gifts of modest value such as gadgets and products expressly approved by TAGETIK SOFTWARE S.R.L. are exceptionally permitted;

c) grant other advantages of any kind (promises of employment, etc.) in favour of representatives of the Public Administration which may give rise to the same consequences as those referred to in point b) above;

d) provide services in favour of business partners which maintain relations with the public administration and which are not adequately justified in the context of the contractual relationship established with such partners;

e) grant remuneration in favour of collaborators who operate in contact with the public administration and which is not adequately justified in relation to the type of engagement to be carried out;

f) submit untruthful, incomplete or partial declarations to national or EU public bodies in order to be awarded public tenders or to obtain contracts from public companies and/or companies with a majority public shareholding, to obtain public disbursements, contributions or subsidised financing or any other outcome;

g) allocate sums received from national or EU public bodies by way of disbursements, contributions or financing to purposes other than those for which they were intended.

The management of every relationship with the Public Administration must be based on the fundamental principles set out in the corporate Code of Ethics and must always have the following characteristics:

- **formality:** the formal procedures laid down by the rules governing administrative proceedings should always be followed and informal — still less confidential — relations with representatives of public administrations should be avoided as far as possible;
- **traceability:** written records must be kept of the main stages and contacts in the course of administrative proceedings;
- **control:** activities involving participation in tenders, the obtaining of contracts and the provision of services to the public administration must be verified in advance and during their performance by the functions responsible and, to the extent necessary, by the Supervisory Body.

5. Principles of conduct in the management of indirect-risk activities

As stated, the Model must provide for further controls over certain areas of activity which may provide the opportunity to set aside sums of money to be used for corrupt purposes, or to confer engagements and advantages which may conceal unlawful payments. In particular:

Participation in public tenders and/or conclusion of contracts with companies with a majority public shareholding Any participation in public tenders, as well as the obtaining of contracts from public companies and/or companies with a majority public shareholding and the related provision of services, must be carried out with scrupulous attention to transparency and compliance with the rules of fairness and truthfulness of declarations.

Payment management activities Payment activities follow a specific internal procedure requiring the involvement and/or authorisation of at least two persons. No invoice, save only for those of negligible amount, may be paid in a manner different from the procedure laid down.

Staff selection Staff selection is carried out by the function concerned in agreement with the Human Resources Manager, in accordance with the relevant internal procedure.

Engagements of external consultants and professionals Engagements of self-employed professionals, consultants and external collaborators are assigned by means of an engagement letter and/or written contract setting out their content and the amount of the fees agreed. The involvement of external consultants and professionals must also provide for prior verification of the supplier, as required by the specific procedure relating to the management of services provided to the Public Administration.

6. Reference internal procedures and documents

The following internal procedures and documents are of reference for this special part:

1. Code of Ethics
2. IT Purchasing Procedure
3. Marketing Purchasing Procedure
4. Goods and Services Purchasing Procedure
5. Sales Agents Management Procedure

6. Sales Procedure
7. Payments and Expense Reimbursements Procedure
8. HR Procedure
9. Procedure for public tenders and the provision of services to the Public Administration
10. SpeakUp policy

These procedures are to be regarded as supplementing and explaining the practices defined in this Special Part.

SPECIAL PART "B" — Computer crimes and unlawful data processing, as well as copyright offences

1. The categories of relevant computer offences (Art. 24-*bis* of the Decree)

Law No. 48 of 2008 ratified and implemented the Council of Europe Convention on Cybercrime, signed in Budapest on 23 November 2001.

Law No. 48 introduced a series of new categories of offence into the Criminal Code.

At the same time, it introduced into the Decree Article 24-*bis*, which established the administrative liability of Entities also in the event of the commission of computer crimes in their interest or to their advantage.

The text of the provision is, in particular, as follows: "(Computer crimes 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, the entity shall be subject to a monetary penalty of between one hundred and five hundred units. 2. In relation to the commission of the offences referred to in Articles 615-*quater* and 615-*quinquies* of the Criminal Code, the entity shall be subject to a monetary penalty of up to three hundred units. 3. In relation to the commission of the offences referred to in Articles 491-*bis* and 640-*quinquies* of the Criminal Code, save as provided for by Article 24 of this decree in cases of computer fraud to the detriment of the State or another public body, the entity shall be subject to a monetary penalty of up to four hundred units. 4. In the event of conviction for one of the offences indicated in paragraph 1, the disqualifying sanctions provided for by Article 9, paragraph 2, letters a), b) and e) shall apply. In the event of conviction for one of the offences indicated in paragraph 2, the disqualifying sanctions provided for by Article 9, paragraph 2, letters b) and e) shall apply. In the event of conviction for one of the offences indicated in paragraph 3, the disqualifying sanctions provided for by Article 9, paragraph 2, letters c), d) and e) shall apply."

A brief description of the offences referred to in this provision is given below.

Unauthorised access to a computer system (Art. 615-*ter* of the Criminal Code) The provision penalises the conduct of a person who, similarly to what occurs in the case of physical trespass, unlawfully accesses or remains, against the express wishes of the person entitled, in a computer system protected by security measures.

Unlawful interception, obstruction or interruption of computer or telematic communications (Art. 617-*quater* of the Criminal Code) The provision refers to the conduct of a person who fraudulently intercepts telematic communications or wilfully interrupts or obstructs them.

Installation of equipment designed to intercept, obstruct or interrupt telematic communications (Art. 617-*quinquies*) The provision, anticipating the protection of the confidentiality of telematic communications, penalises the mere installation of equipment designed to intercept, even where it is not followed by any actual interception, interruption or obstruction.

Categories of damage (Arts. 635-*bis* – 635-*quinquies* of the Criminal Code) Articles 635-*bis* et seq. penalise a complex series of categories whose common element is conduct involving the wilful damaging of computer data and systems.

Article 635-*bis* first penalises the wilful damaging of computer programs or data. The provision indeed penalises anyone who destroys, impairs, deletes, alters or suppresses another's computer information, data or programs, with imprisonment from six months to three years.

Article 635-*ter* punishes more severely anyone who commits an act aimed at destroying, impairing, deleting, altering or suppressing information, data or computer programs used by the State or by another public body or pertaining to them, or in any event of public utility.

Article 635-*quater* penalises the damaging of computer or telematic systems and, in particular, the conduct of a person who, engaging in one of the forms of conduct referred to in Article 635-*bis* aimed at damaging programs and data, damages more generally the functioning of an entire computer system.

Article 635-*quinquies* punishes still more severely the acts referred to in the preceding article where they relate to systems of public utility.

Unlawful possession and dissemination of access codes to computer or telematic systems (Art. 615-*quater* of the Criminal Code) The provision penalises the conduct of a person who, in order to obtain a profit or cause damage, disseminates, communicates, delivers, reproduces or procures codes, passwords or other means capable of allowing access to a computer system protected by security measures.

Dissemination of programs designed to damage or interrupt a computer system (Art. 615-*quinquies* of the Criminal Code) The provision penalises the conduct of a person who disseminates so-called computer viruses, that is to say programs designed to enter computer systems and to prevent or damage their operation or to bring about the destruction of the data contained therein.

Forgery of computer documents (Art. 491-*bis* of the Criminal Code) The provision in question extends the categories of offence provided for by the chapter dedicated to forgery of documents to cases in which they are committed in respect of computer documents.

Computer fraud by a provider of electronic signature certification services (Art. 640-*quinquies* of the Criminal Code) The article penalises the conduct of a provider of electronic signature certification services who, in order to procure for themselves or for others an unjust

profit or to cause damage to others, breaches the obligations laid down by law for the issue of a qualified certificate.

As regards copyright, Law 99/09 of 23 July 2009, "Provisions for the development and internationalisation of undertakings, as well as in the field of energy", introduced into Legislative Decree 231/01 the following provision:

("Offences relating to breach of copyright") In relation to the commission of the offences provided for by Articles 171, first paragraph, letter a-bis), and third paragraph, 171-*bis*, 171-*ter*, 171-*septies* and 171-*octies* of Law No. 633 of 22 April 1941, the entity shall be subject to a monetary penalty of up to five hundred units.

2. In the event of conviction for the offences referred to in paragraph 1, the disqualifying sanctions provided for by Article 9, paragraph 2 shall apply to the entity for a period not exceeding one year. The provisions of Article 174-*quinquies* of the aforementioned Law No. 633 of 1941 remain unaffected.

A brief description of the offences referred to in this provision is given below.

Dissemination, in whole or in part, of a protected intellectual work through the use of telematic networks (Art. 171, first paragraph, letter a-bis, of Law 633/1941) The offence in question arises where a person infringes copyright by disseminating — through the use of telematic networks — protected intellectual works, in whole or in part.

Unlawful handling of computer programs and protected databases (Art. 171-*bis* of Law 633/1941) The offence in question arises where, for the purpose of profit, conduct is engaged in aimed at unlawfully duplicating, importing, distributing, selling, leasing, disseminating/transmitting to the public, or holding for commercial purposes — or in any event for profit — computer programs and the contents of protected databases.

Unlawful handling of works of literary, musical, multimedia, cinematographic or artistic content (Art. 171-*ter* of Law 633/1941) The offence in question arises where, for gain, conduct is engaged in aimed at unlawfully duplicating, importing, distributing, selling, renting, disseminating/transmitting to the public, or holding for commercial purposes — or in any event for profit — any work protected by copyright and related rights, including works of literary, musical, multimedia, cinematographic or artistic content.

Improper handling of media exempt from marking obligations or fraudulent failure to comply with marking obligations (Art. 171-*septies* of Law 633/1941) The offence in question arises where producers or importers of media not subject to the SIAE mark fail to communicate to that body, within thirty days of the date of placing on the market in the national territory or of importation, the data necessary for the unequivocal identification of those media, or where such persons falsely declare that they have complied with the marking obligations.

Unlawful or otherwise fraudulent handling of devices for the decoding of conditional-access audiovisual transmissions (Art. 171-*octies* of Law 633/1941) The offence in question arises where, for fraudulent purposes, conduct is engaged in aimed at producing, offering for sale, importing, promoting, installing, modifying, or using for public and private use, devices or parts of devices designed for the decoding of conditional-access audiovisual transmissions carried out over the air, by satellite or by cable, in either analogue or digital form.

2. Risk areas

In the abstract, all activities of persons who, within the scope of their corporate duties, access and make use of the computer network are to be regarded as risk areas.

In concrete terms, the type of criminal offences under examination makes it possible to limit the potential unlawful activities in the interest of TAGETIK SOFTWARE S.R.L. or of its subsidiaries to the following activities:

- alteration and falsification of public or private electronic documents;
- espionage or sabotage activities carried out by computer means and directed at competitors, whether public or private (creation, modification, alteration of another's data; unauthorised access to another's systems; unauthorised modification of another's programs and their damaging; unlawful possession of passwords for access to another's systems; fraudulent interception of another's computer communications; installation of devices intended for such unlawful activity; dissemination of viruses, etc.);
- the distribution of software without the necessary licences and, consequently, breach of copyright rules.

Given the nature of the TAGETIK SOFTWARE S.R.L. companies, which operate primarily (and almost exclusively) in the IT sector, as well as in direct contact with Databases and, in general, with clients' IT infrastructure, the occurrence of offences in such areas has been assessed as relevant in the course of risk analysis and mapping.

3. Rules of conduct and procedures

In general, all Addressees:

- must use the corporate computer network exclusively for professional purposes, operations and communications;
- must access, connect to and exchange data with third-party computer networks only for professional reasons, in the cases and for the time strictly necessary;
- must protect the client data of which they may come into possession for reasons relating to the development of activities and must maintain the strictest confidentiality in respect of such data in accordance with the confidentiality agreements entered into with the client company, including after the end of the commercial relationship with that client;
- must protect IT tools, corporate data and client data in every situation, including in respect of any activities carried out at clients' premises, as well as the use and protection of laptops and other mobile devices;
- must avoid using software and, more generally, computer programs in breach of copyright rules;
- must report to the IT Manager and/or to Company Management any fact, event or anomaly which may give rise to a well-founded suspicion that computer abuse is taking place.

With reference to the type of offences covered by this Special Part, their effective prevention can and must be based on two points:

- the certain identification of the identity of the person who from time to time accesses and operates on the computer network;
- appropriate measures to prevent access to the network by third parties and unauthorised persons, so as to exclude the possibility that anyone may act anonymously on the corporate computer network;
- the periodic verification of the lawfulness of the software installed on PCs and on the corporate computer network.

On these points, it should be noted that TAGETIK SOFTWARE S.R.L. voluntarily maintains a Security Policy Document and has adopted an Information Security Management System pursuant to standard UNI CEI ISO/IEC 27001:2013 (certified by the third-party body ISONIKE), setting out all the security measures designed to prevent unauthorised access (whether physical or logical) to the sensitive data processed by the company: this Special Part refers to those measures, documents and systems (insofar as they are compatible with the aspect of access to and security of the computer network), making them an integral part of this Model as well.

Furthermore, Managing Directors with specific powers in relation to data protection have been identified at Divisional level, respectively for the consultancy phases and the software development phases.

4. Reference internal procedures and documents

The following internal procedures and documents are of reference for this special part:

- All procedures and documents of the information security management system pursuant to standard UNI CEI ISO/IEC 27001:2013
- Security Policy Document
- Corporate IT Regulations

These procedures and documents are to be regarded as supplementing and explaining the practices defined in this Special Part.

SPECIAL PART "C" — Corporate offences

1. Introduction

Legislative Decree No. 61 of 2002 reformed the area of so-called corporate offences, reformulating Articles 2621 et seq. of the Civil Code. That same decree introduced into the text of the Decree Article 25-*ter*, which extended the applicability of the administrative liability of Entities also to the commission of "corporate offences provided for by the Civil Code, if committed in the interest of the company by directors, general managers or liquidators or by persons subject to their supervision, where the act would not have occurred had they exercised supervision in accordance with the obligations inherent in their office".

2. The categories of Corporate offences

A brief description is given below of the principal offences relevant for the purposes of this Second Special Part.

2.1 CATEGORIES OF FALSIFICATION

False corporate communications (Arts. 2621 and 2622 of the Civil Code) The categories outlined in Articles 2621 and 2622 of the Civil Code are intended to penalise the presentation, in the corporate communications required by law, of false information, or the omission of information which is due, by directors, general managers, statutory auditors and liquidators, in such a way as to mislead the addressees of those communications. For the conduct to be criminally relevant, it must be engaged in with the twofold intention of deceiving the shareholders, creditors or the public, on the one hand, and of obtaining for oneself or for others an unjust profit, on the other.

False statements in prospectuses (Art. 2623 of the Civil Code) The category identified by Article 2623 is intended to protect the truthfulness and completeness of information addressed to the market, in cases where the company wishes to solicit investment or intends to proceed with a listing on regulated markets or with public purchase or exchange offers. The provision indeed penalises the conduct of a person who, on such occasions, disseminates false information, or conceals true information, with the intention of misleading the public. In this case too, as in the previous one, the conduct must not only be directed at deceiving the addressees of the information but must also aim to produce an unjust profit for the perpetrator or for other persons. Here again, the offence constitutes a contravention or a crime depending on whether or not the conduct has caused financial damage to the addressees of the information prospectus.

False statements in the reports and communications of the auditing firm (Art. 2624 of the Civil Code) In this case, what is protected is the truthfulness and completeness of the communications of persons entrusted with the statutory audit of the company. As above, where the conduct has resulted in financial damage to the addressees of the communications, the penalty is aggravated and the offence ceases to be a contravention and becomes a crime. The offence referred to in Article 2624 is a special-subject offence, capable of being committed by persons responsible for the statutory audit; this does not preclude directors and all other persons referred to in Article 25-*ter* of the Decree from being involved as accomplices.

2.2 PROTECTION OF SHARE CAPITAL

Undue return of contributions (Art. 2626 of the Civil Code) The provision is breached where, outside cases of lawful reduction of share capital, contributions are returned, including in a simulated manner, to one or more shareholders, or one of them is released from the obligation to make them.

Unlawful distribution of profits or reserves (Art. 2627 of the Civil Code) The conduct identified by the provision arises where profits or interim dividends on profits which have not actually been earned, or which are allocated by law to reserves, are distributed, or where another reserve which by law may not be distributed is distributed. The provision nonetheless provides that the return of the profits or the reconstitution of the reserves before the deadline for the approval of the financial statements extinguishes the offence.

Unlawful transactions in shares or quotas of the company or of the parent company (Art. 2628 of the Civil Code) The offence is completed by the purchase or subscription of shares or quotas of the company or of the parent company which impairs the integrity of the share capital or of non-distributable reserves. As in the case of unlawful distribution of profits, the reconstitution of the share capital or of the reserves before the deadline for the approval of the financial statements extinguishes the offence.

Transactions prejudicial to creditors (Art. 2629 of the Civil Code) This category protects the security of creditors and prohibits the carrying out of transactions such as a reduction of capital, a merger with another company or a demerger, where these cause damage to the company's creditors. Where, before judgment, compensation for the damage suffered by them is provided, the offence is extinguished.

Failure to disclose a conflict of interest (Art. 2629-*bis* of the Civil Code) The provision was introduced by Law 262/2005 containing the "Provisions for the protection of savings and the regulation of financial markets". Article 2629-*bis* of the Civil Code provides for breach of Article 2391, first paragraph, of the Civil Code (which lays down the obligation to disclose a conflict of interest) committed by the directors of a company with securities admitted to trading on regulated markets or widely distributed among the public, or by a person subject to supervision under the TUF.

Fictitious formation of capital (Art. 2632 of the Civil Code) The provision covers three possible forms of conduct, sharing the same effect of bringing about the formation of fictitious capital: - the allocation of company quotas or shares for a sum lower than their nominal value; - the reciprocal subscription of shares or quotas; - the significant overvaluation of contributions in kind, of receivables, or of the company's assets in the event of a transformation.

Undue distribution of corporate assets by liquidators (Art. 2633 of the Civil Code) This category concerns the case where, during liquidation, the liquidators distribute corporate assets among the shareholders before paying creditors or setting aside the sums necessary to satisfy them, thereby causing damage to those creditors. The offence is extinguished if, before judgment, compensation is provided.

2.3 PROTECTION OF THE PROPER FUNCTIONING OF THE COMPANY

Obstruction of control (Art. 2625 of the Civil Code) The offence consists in hindering the control activities which the law attributes to certain persons — shareholders, corporate bodies, any auditing firm — through the concealment of documents or other suitable artifices. Where damage is actually caused, the penalty is aggravated.

Private-sector bribery (Art. 2635 of the Civil Code) The offence consists in the giving of money and/or benefits (including a mere promise) which entails a breach of duties of office or of loyalty, causing damage to the company.

Unlawful influence on the shareholders' meeting (Art. 2636 of the Civil Code) The provision identifies and penalises the conduct of a person who, by simulated acts or by fraud, determines the formation of the majority at a shareholders' meeting, in order to procure for themselves or for others an unjust profit.

2.4 PROTECTION AGAINST FRAUD

Market rigging (Art. 2637 of the Civil Code) The category provided for by Article 2637 is constituted by the conduct of a person who disseminates false information or engages in simulated transactions or other artifices concretely capable of significantly influencing the price of unlisted financial instruments or of significantly affecting public confidence in the financial soundness of banks or banking groups. It should be expressly emphasised that, as from 2005, the provision penalises only market-rigging conduct affecting the value of unlisted securities. From that year, indeed, the legislator introduced Articles 184 and 185 into the TUF, separately regulating market abuse in respect of the securities of listed companies. That same law introduced a new Article 25-*sexies* into the Decree, expressly providing for the administrative liability of Entities also in respect of these two new categories of offence. Special Part "D" below is dedicated to these two categories of market abuse.

2.5 PROTECTION OF PUBLIC SUPERVISORY FUNCTIONS

Obstruction of the exercise of the functions of public supervisory authorities (Art. 2638 of the Civil Code) The provision covers two different forms of conduct, distinguished by their manner and by the moment of the offence. The first consists either in the presentation of material facts which do not correspond to the truth as regards the balance-sheet, economic and financial position, even if subject to valuation, in the communications required by law to Public Supervisory Authorities, or in the concealment of facts, likewise relating to the economic, balance-sheet and financial position, which ought to have been communicated. The second consists in any other form of obstruction, knowingly carried out, of the supervisory activities of the Public Authorities.

3. Risk Areas

In the light of the offences and conduct referred to above, the analysis of TAGETIK SOFTWARE S.R.L.'s business activities has revealed the existence of a modest risk of commission of the corporate offences described.

TAGETIK SOFTWARE S.R.L. is not a listed company, does not raise funds from the public and is not subject to the relevant Public Supervisory Authority (CONSOB): these factors exclude the existence of a specific risk of commission of those of the unlawful acts indicated which relate to these aspects (prospectuses, relations with the market, relations with Supervisory Authorities).

The risks of commission of corporate unlawful acts are therefore connected with those inherent in any legal person carrying on a business and are, in particular, identifiable in the following areas of activity:

A) the preparation of communications addressed to shareholders or to the public and, in particular, the drafting and preparation of the annual financial statements; in this case too, however, it should be emphasised that the shareholders substantially coincide with the directors, and therefore this category of offence is likewise reduced;

B) transactions affecting share capital and the management of corporate governance;

C) commercial promotion activities and the management of business relations generally, including between private parties.

The list is open to future additions; it will therefore always be possible to identify further risk areas (with the consequent preparation of specific rules of conduct and related procedures).

In this regard, the Supervisory Body may propose to the Board of Directors any appropriate amendment to the text of this Special Part. The Board of Directors may, moreover, take analogous initiatives on its own initiative.

In addition to the specific indications and principles of conduct set out below, reference is also made to all the principles generally accepted by TAGETIK SOFTWARE S.R.L. as well as by the General Part of this Model.

4. General rules of conduct

The Addressees are expressly required:

- to behave in a proper, scrupulously transparent and cooperative manner, in compliance with statutory rules and with all corporate procedures, in all activities connected with and aimed at the preparation of the financial statements and other corporate communications, with the aim of always providing shareholders and third parties with truthful, complete and accurate information on the economic, financial and balance-sheet position of TAGETIK SOFTWARE S.R.L. as a whole;
- to exercise the utmost care and caution, through compliance with statutory rules and with the internal procedures addressed to them, in protecting the integrity and effectiveness of the share capital and corporate assets, in full compliance with the safeguards of creditors and third parties generally;
- to take care of and protect the proper functioning of the corporate bodies of TAGETIK SOFTWARE S.R.L., guaranteeing and facilitating every form of control over corporate management and ensuring the free formation of the will of the shareholders' meeting;
- to ensure that all communications required by the applicable rules towards the competent Authorities are made truthfully, promptly and correctly, avoiding placing any obstacle in the way of the exercise of their control and verification activities;
- not to disclose information regarding the initiatives and choices of business partners (conclusion of agreements by TAGETIK SOFTWARE S.R.L., collaborations with the Company and so on), except where strictly necessary and with the agreement of the partner concerned;
- to implement ethical practices in business relations designed to avoid the possible offence of private-sector bribery.

5. Specific rules of conduct relating to the individual Risk areas

5.1 Communications to Shareholders and to the public

Financial statements and other corporate communications TAGETIK SOFTWARE S.R.L. has developed a specific procedure for the preparation of its annual financial statements, identifying all the corporate functions and therefore the persons who must contribute to that activity. The

Functions involved are: - group administration; - directors of the Italian and foreign companies; - external tax adviser.

The Company is also equipped with a scrupulous control system which makes it possible to monitor, in real time, the accounting position of TAGETIK SOFTWARE S.R.L., and therefore allows it to be considered that, in this respect, the risk of commission of any of the offences under examination is greatly reduced.

5.2 Protection of Share Capital

All transactions which may, even indirectly, affect the share capital of TAGETIK SOFTWARE S.R.L., such as in particular the acquisition or disposal of shareholdings or business divisions, mergers, demergers or spin-offs, must provide for:

- the precise allocation of decision-making and operational responsibilities within individual projects, as well as the mechanisms for coordination between the functions thus identified;
- information to the Supervisory Body from the outset of the project, so that it may follow the entire decision-making process;
- the making available to the Supervisory Body of all documentation relating to each project.

As regards any conflict of interest, directors are required to communicate to the Board of Directors and to the Supervisory Body, which sees to its filing and updating, all information relating to offices held or shareholdings held, directly or indirectly, in other companies or undertakings, as well as the cessation or modification thereof, which, by their nature or type, may reasonably give rise to conflicts of interest within the meaning of Article 2391 of the Civil Code.

5.3 Relations with the competent Authorities

As regards any relations with the competent Authorities, there are three potentially relevant areas of activity:

- the preparation and transmission of information, whether periodic or not, required by law and by regulations;
- the preparation and transmission of any other information further requested by the competent Authorities;
- the conduct to be adopted in the event of inspections by those Authorities.

In such cases, activities must be governed by the following principles:

- the timing and manner of transmission and internal circulation of the data necessary for the preparation of information to the competent Authorities, with the provision of mechanisms and procedures ensuring the maximum truthfulness and completeness thereof;
- the identification of persons responsible for ensuring compliance with the procedures laid down and for issuing a declaration of the truthfulness and completeness of the information collected and prepared;

- in the event of inspections, the fullest cooperation on the part of all corporate units involved, the prompt identification of a person responsible for the necessary activities, capable of ensuring the maximum coordination between the corporate units involved and the maximum speed in making available the information requested by the inspectors;
- in general, the possibility, for all the identified responsible persons, to approach and report to the Supervisory Body regarding the conduct of activities relating to relations with the competent Authorities, also reporting any shortcomings in the procedures and operating methods put in place;
- as regards the person identified in the event of inspections, the drafting of a report to the Supervisory Body on the investigation commenced, which must be periodically updated in relation to developments in the investigation itself and to its outcome.

6. Reference internal procedures and documents

The following internal procedures and documents are of reference for this special part:

1. Code of Ethics
2. Financial Statements Preparation Procedure
3. Sales Procedure

These procedures and documents are to be regarded as supplementing and explaining the practices defined in this Special Part.

SPECIAL PART "D" — Market abuse

1. The offences referred to in Articles 184 and 185 of the TUF (Art. 25-*sexies* of the Decree)

Article 9 of Law No. 62 of 18 April 2005, implementing the requirements of Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003, introduced Article 25-*sexies* into the Decree. That provision extends the scope of application of the rules on the administrative liability of Entities also to conduct by corporate representatives constituting one of the two categories of market abuse provided for in the TUF.

That same law redefined the framework of market abuse offences, introducing two distinct crimes in Articles 184 and 185 of the TUF.

Article 184 penalises so-called insider dealing with imprisonment from two to twelve years and a fine of between forty thousand and six million euro: the offence arises where a person, being in possession of inside information by reason of their capacity as a member of the administrative, management or supervisory bodies of the issuer, or of their shareholding in the issuer's capital, or of the exercise of an employment, a profession or a function, including a public one, or of an office, 1) carries out transactions in financial instruments using that information, or 2) discloses that information to others, or 3) recommends or induces others to carry out transactions.

Under paragraph 2 of the provision, the same offence may be committed by any person who, although lacking one of the capacities indicated in the first paragraph, has come into possession of sensitive information by reason of the preparation of an offence.

Article 181 of the TUF also expressly defines the notion of inside information: this means information of a precise nature, which has not been made public, relating, directly or indirectly, to one or more issuers of financial instruments or to one or more financial instruments, and which, if made public, could significantly affect the prices of those financial instruments.

Information is deemed to be of a precise nature if: i) it refers to a set of circumstances which exists or which may reasonably be expected to come into existence, or to an event which has occurred or which may reasonably be expected to occur; ii) it is sufficiently specific to enable conclusions to be drawn as to the possible effect of the set of circumstances or event referred to in point a) on the prices of financial instruments.

Information which, if made public, could significantly affect the prices of financial instruments means information which a reasonable investor would be likely to use as one of the bases of their investment decisions.

Article 185 of the TUF, by contrast, penalises conduct amounting to market manipulation.

That provision, in particular, penalises with imprisonment from two to twelve years and a fine of between forty thousand and ten million euro, three types of conduct:

1) the dissemination of false information;
2) the carrying out of simulated transactions;
3) the use of other artifices;

where such conduct is capable of causing a significant alteration in the price of listed financial instruments.

2. Risk areas

TAGETIK SOFTWARE S.R.L. is not a listed company: this eliminates the risk that, in the course of its activities, market abuse relating to the securities of that same company may be committed. Furthermore, TAGETIK SOFTWARE S.R.L. does not hold shareholdings in listed companies and does not operate on the stock market.

By contrast, the management of information relating to client companies which are listed must be considered as a risk area: in the course of their daily activities, TAGETIK SOFTWARE S.R.L.'s consultants are in direct contact with data relating to the financial statements and/or group consolidated accounts of leading companies listed on the Italian and foreign stock exchanges.

The areas of the Company considered most at risk of the commission of market abuse activities are identifiable as follows:

a. the management of information relating to any relationships with listed clients or clients connected with other listed parties, prior to their formalisation/official announcement;

b. communication activities relating to new agreements, new services and new partnerships involving listed clients or clients connected with listed third parties.

3. General rules of conduct

As an expressly formalised general rule, all information relating to the management of the business, to clients, to financial statement data, to the conclusion of agreements and so forth must be treated and managed as confidential information and disseminated only among those persons strictly necessary and involved in the specific project activities.

With specific reference to consultancy activities, TAGETIK SOFTWARE S.R.L. lays down the following rules of conduct:

- every form of communication with third parties must be based on principles of the utmost confidentiality;
- every consultant taking part in projects in the course of which inside information may be received or made available must have signed in advance a general confidentiality undertaking and a specific undertaking to protect client data encountered during project activities;
- all Addressees are required to report promptly any conduct and any fact which may suggest the exploitation or disclosure of confidential information, if not indeed the commission of market abuse.

4. Reference internal procedures and documents

The following internal procedures and documents are of reference for this special part:

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

These procedures and documents are to be regarded as supplementing and explaining the practices defined in this Special Part.

SPECIAL PART "E" — Offences in breach of occupational health and safety rules

1. Manslaughter and serious or very serious personal injury in breach of occupational health and safety rules (Art. 25-*septies* of the Decree)

Article 25-*septies* of the Decree, introduced by Law No. 123 of 23 August 2007 and replaced by Article 300 of Legislative Decree 81/2008 (the so-called Consolidated Act on the protection of health and safety in the workplace), extended the administrative liability of the Entity also to the offences of manslaughter and serious or very serious personal injury committed in breach of occupational health and safety rules.

In this regard, it should be noted that the aforementioned decree, in addition to reforming and systematically reorganising the extensive body of rules on the protection of health and safety in

the workplace, extended the administrative liability of the entity to the offences under examination and laid down certain specific rules regarding the preparation of the Model.

Manslaughter (Art. 589 of the Criminal Code) Anyone who negligently causes the death of a person shall be punished with imprisonment from six months to five years. If the act is committed in breach of the rules governing road traffic or of those on accident prevention at work, the penalty is imprisonment from two to seven years. In the event of the death of several persons, or of the death of one or more persons and injury to one or more persons, the penalty which would be imposed for the most serious of the breaches committed shall apply, increased up to threefold, but the penalty may not exceed fifteen years.

Negligent personal injury (Art. 590 of the Criminal Code) Anyone who negligently causes personal injury to another shall be punished with imprisonment of up to three months or a fine of up to EUR 309. If the injury is serious, the penalty is imprisonment from one to six months or a fine of between EUR 123 and EUR 619; if it is very serious, imprisonment from three months to two years or a fine of between EUR 309 and EUR 1,239. If the acts referred to in the second paragraph are committed in breach of the rules governing road traffic or of those on the prevention of accidents at work, the penalty for serious injury is imprisonment from three months to one year or a fine of between EUR 500 and EUR 2,000, and the penalty for very serious injury is imprisonment from one to three years. In the event of injury to several persons, the penalty which would be imposed for the most serious of the breaches committed shall apply, increased up to threefold; but the term of imprisonment may not exceed five years. The offence is prosecutable upon complaint by the injured party, save in the cases provided for in the first and second sub-paragraphs, limited to acts committed in breach of the rules on the prevention of accidents at work or relating to occupational hygiene which have caused an occupational disease.

*****

It should be made clear that not all instances of manslaughter or serious or very serious negligent personal injury can constitute the basis for administrative liability: indeed, pursuant to Article 25-*septies* under examination, only those acts are relevant in which the negligent conduct which caused the harm to a person's physical integrity consisted in the failure to comply with one or more statutory or regulatory rules laid down for the protection of health and safety at work.

It is also necessary to specify that, pursuant to Article 583, paragraph 1 of the Criminal Code, personal injury is to be considered "serious" if: (i) the act results in an illness which endangers the life of the injured party, or an illness or an incapacity to attend to ordinary occupations for a period exceeding 40 days; (ii) the act produces the permanent weakening of a sense or of an organ.

Injury is instead considered "very serious", pursuant to the same Article 583, paragraph 2 of the Criminal Code, if the act results in: (i) an illness which is certainly or probably incurable; (ii) the loss of a sense; (iii) the loss of a limb, or a mutilation rendering the limb unusable, or the loss of the use of an organ or of the capacity to procreate, or a permanent and serious difficulty of speech; (iv) disfigurement, or permanent scarring of the face.

As regards the sanctioning regime introduced by the Decree in relation to the offences under examination, three different degrees of gravity of the unlawful act, and therefore of the sanction applicable to the entity, are distinguished. In particular:

(i) in the case of manslaughter resulting from the most serious breaches indicated in Article 55, paragraph 2 of the Consolidated Act (consisting, in summary, in the failure to draw up, or the inadequate drafting of, the risk assessment document required by law in undertakings whose activities are characterised by particular hazard), the monetary penalty is 1,000 units; disqualifying sanctions range from a minimum of three months to a maximum of one year;

(ii) in the case of manslaughter committed in breach of occupational health and safety rules, the monetary penalty ranges from 250 to 500 units; disqualifying sanctions from a minimum of three months to a maximum of one year;

(iii) in the case of serious or very serious negligent injury, the maximum monetary penalty is 250 units; disqualifying sanctions do not exceed six months.

*****

2. Addressees of this special part

In view of the purpose of the categories of offence under examination, it is entirely clear that every business activity constitutes a risk in this respect, both for those who carry it out and for the community in general.

An immediate consequence of these premises is that, in addition to the Addressees of the Model, the following must be regarded as addressees of this Special Part:

- all persons who perform functions and hold roles in matters of occupational health and safety (by way of example, the employer's delegates, safety officers, competent physicians, emergency response personnel, etc.);
- external service providers operating within the corporate premises;
- workers of contracting undertakings operating within the corporate premises;
- other collaborators, including occasional ones;
- visitors to the offices and other corporate areas.

3. Purpose of this special part

It should first be noted that the crimes covered by this Special Part, unlike all the others provided for by the Decree, do not consist in intentional unlawful conduct; they are constituted by merely negligent, and therefore involuntary, conduct.

In the case of negligent injury, therefore, no one pursues the occurrence of the harmful event: it occurs by reason of a prior omission as regards compliance with accident-prevention rules determined by fault (that is, by negligence, imprudence or lack of skill), and certainly not by the will to cause the event.

This Special Part therefore has the purpose of preventing this type of offence, through the provision of a series of internal organisational measures aimed at the punctual and exhaustive adoption of all the remedies and all the measures imposed by law and by regulations for the full protection of safety at work and the minimisation of the risk that omissions and shortcomings may occur in this area of activity.

In pursuing prevention objectives, Article 30 of Legislative Decree 81/2008 specifies that the Organisational Model, in relation to the specific offences referred to in Article 25-*septies*, must be designed to ensure:

a) compliance with the technical and structural standards laid down by law relating to equipment, plant, workplaces, chemical, physical and biological agents;
b) risk assessment activities and the preparation of the consequent prevention and protection measures;
c) activities of an organisational nature, such as emergencies, first aid, contract management, periodic safety meetings, consultation of workers' safety representatives;
d) health surveillance activities;
e) worker information and training activities;
f) supervisory activities with reference to compliance by workers with safe working procedures and instructions;
g) the acquisition of documentation and certifications required by law;
h) periodic verification of the application and effectiveness of the procedures adopted.

It should, by contrast, be noted that in the specific reality of TAGETIK SOFTWARE S.R.L., whose structure consists substantially of offices and of workers carrying out predominantly intellectual activities, the risks of offences under the aforementioned Article 25-*septies* are decidedly limited although, clearly, not excludable.

This Model therefore expressly aims to:

- provide measures and methods suitable for monitoring the application of the activities required by Legislative Decree 81/2008 as amended in relation to the mandatory obligations applicable to the reality of TAGETIK SOFTWARE S.R.L.;
- provide for the extension of the existing disciplinary system also to shortcomings, omissions and breaches in accident-prevention matters.

4. Persons entrusted with safety-related tasks

The persons who play a significant role in the protection of occupational health and safety are:

1. The Employer, in respect of the tasks which may not be delegated;
2. The Head of the Prevention and Protection Service (RSPP);
3. Fire-fighting and first-aid personnel;
4. Supervisors responsible for compliance with safety rules;
5. The Workers' Safety Representative (RLS);
6. The Competent Physician;
7. Workers.

For the purposes of occupational health and safety, the Employer has been identified and specifically delegated by the Board of Directors from among the Managing Directors of the Company. It is for that person to fulfil their non-delegable tasks with reference first and foremost to the risk assessment and to the appointment of the company Head of the Prevention and Protection Service (RSPP), currently identified as an external consultant who works alongside the company and who has accepted that role in a personal capacity.

Workers assigned to the fire-fighting service and workers assigned to the first-aid service have also been identified, having attended the relevant training and/or periodic refresher courses, and the Competent Physician has been appointed.

To the persons referred to so far must finally be added all workers: the contribution of knowledge and information regarding safety risks from all persons involved in the undertaking's activities is indeed fundamental to an internal system aimed at the most effective possible protection of safety, including with reference to the most rapid and prompt detection of any shortcomings, any gaps and any need for adaptation in the event of organisational changes.

5. Planning and organisation of the System

In order to give concrete effect to the principles of its safety management, TAGETIK SOFTWARE S.R.L. has adopted a specific occupational health and safety management system pursuant to the international standard UNI EN ISO 45001:2023 and has obtained certification thereof from the third-party body ISONIKE.

6. Assessment of existing risks

A necessary and essential prerequisite for effective activity to prevent risks to occupational health and safety is an effective, adequate and continuous identification and assessment of the health and safety risks existing within the corporate organisation.

The fundamental resulting document is the Risk Assessment Document provided for by the Consolidated Act. It is drawn up, updated and refined by the Employer with the technical support of the RSPP.

That document is accompanied by further and more specific documents, relating to particular types of risk such as, first and foremost, the fire risk assessment and the work-related stress risk assessment.

In the light of the outcomes of the occupational health and safety risk assessments, TAGETIK SOFTWARE S.R.L. has implemented the necessary risk-reduction measures aimed at preventing accidents and occupational diseases, as well as adopting the procedures defined in the health and safety management system.

Another fundamental aspect is the assessment of any health risks. In this regard, a fundamental role is of course played by the Competent Physician and by the medical documentation archive. Health documentation is retained, in compliance with privacy legislation, in dedicated corporate archives.

The Competent Physician draws up each year a report on their activities, reporting any particular pathologies or accident events which had a particular impact in the preceding year.

7. Particular and/or extraordinary cases in relation to ordinary corporate activity

A further decisive element for effective prevention is that it should base its measures and initiatives not only on an examination of ordinary activity, but also on cases and situations falling outside it: it is precisely those cases in which the persons involved do not belong directly to the Company's organisation, or which concern situations broadly amounting to emergencies, that

carry the greatest risks of activities proving hazardous or of a lowering of the level of precautionary measures.

For this reason, TAGETIK SOFTWARE S.R.L. has also regulated health and safety matters in the case of contracts awarded to third-party undertakings.

8. Information and training

A fundamental aspect of effective activity to protect occupational health and safety consists in the proper training and information of workers and of every other interested party on health and safety matters in the workplace.

TAGETIK SOFTWARE S.R.L., with the support of the RSPP, establishes the forms and methods for ensuring:

1. the effective training and information of workers and of all other persons involved in corporate activities;
2. the contribution of knowledge and experience from workers, who are engaged on a daily basis in the operations and corporate activities.

As regards the first point, the following activities have already been provided for and expressly regulated, also in relation to the mandatory obligations in this area:

- collective training on a periodic or specific basis;
- individual training, on joining the company and in the event of a change of duties;
- access by all interested parties to the safety documentation archive.

As regards the second point, TAGETIK SOFTWARE S.R.L. provides for forms of involvement on the basis of worker training and information activities, of which written evidence must be provided, on a dedicated form, which must be signed by the worker concerned;

- periodic meetings with workers and their representatives;
- the possibility of reporting malfunctions and shortcomings.

Reports of malfunctions may be addressed to the Head of the Prevention and Protection Service (RSPP).

9. Reference internal procedures and documents

The following internal procedures and documents are of reference for this special part:

1. All procedures of the occupational health and safety management system pursuant to standard UNI ISO 45001:2023
2. The corporate Risk Assessment Document (and related occupational health and safety documents)

This system of procedures and documents is to be regarded as supplementing and explaining the practices defined in this Special Part.

SPECIAL PART "F" — Offences relating to receiving stolen goods, money laundering and the use of money, goods or other benefits of unlawful origin, as well as self-laundering

The offences referred to in Article 25-*octies* were introduced into Legislative Decree 231/01 by Legislative Decree No. 231 of 21 November 2007, "Implementation of Directive 2005/60/EC concerning the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, as well as of Directive 2006/70/EC laying down implementing measures". It follows that the purpose of Decree No. 231/2007 is to protect the financial system from being used for the purposes of money laundering or terrorist financing.

These are offences punishable by both monetary and disqualifying sanctions.

The monetary penalty ranges from a minimum of 200 to a maximum of 1,000 units.

In the event of conviction, the disqualifying sanctions provided for by Article 9, paragraph 2 of Legislative Decree 231/2001 also apply to the entity for a period not exceeding two years.

Receiving stolen goods (Art. 648 of the Criminal Code) The offence of receiving stolen goods is committed by anyone who, in order to procure for themselves or for others a profit, purchases, receives or conceals money or goods deriving from any crime in the commission of which they did not participate, or in any event acts as an intermediary in having them purchased, received or concealed. This offence requires specific intent on the part of the person acting, namely the awareness and the will to derive a profit, for themselves or for others, from the purchase, receipt or concealment of goods of criminal origin. Knowledge of the criminal origin of the money or goods is also required; the existence of that mental element may be recognised in the presence of serious and unequivocal circumstances — such as, for example, the quality and characteristics of the goods, the unusual economic and contractual conditions of the transaction, the status or profession of the possessor of the goods — from which it may be inferred that the person who acted could have formed the certainty of the unlawful origin of the money or goods.

Money laundering (Art. 648-*bis* of the Criminal Code) This offence arises where the perpetrator, not having been an accomplice in the commission of the underlying crime, substitutes or transfers money, goods or other benefits deriving from an intentional crime, or carries out other transactions in relation thereto, in such a way as to hinder the identification of their criminal origin. The provision is to be interpreted as being aimed at punishing those who — being aware of the criminal origin of money, goods or other benefits — carry out the conduct described in such a way as to create in practice difficulties in discovering the unlawful origin of the goods concerned. It is not required, for the completion of the offence, that the person acted in order to obtain a profit or with the aim of assisting the perpetrators of the underlying offence in securing its proceeds. Money laundering consists of dynamic conduct, capable of putting the goods into circulation, whereas mere receipt or concealment could constitute the offence of receiving stolen goods.

Use of money, goods or benefits of unlawful origin (Art. 648-*ter* of the Criminal Code) The criminal conduct consists in the use in economic or financial activities of money, goods or other benefits deriving from a crime, outside cases of complicity in the underlying offence and the cases provided for by Articles 648 (receiving stolen goods) and 648-*bis* (money laundering) of the

Criminal Code. As compared with the offence of money laundering, although the same mental element of knowledge of the unlawful origin of the goods is required, Article 648-*ter* confines the conduct to the use of such resources in economic and financial activities. Moreover, in view of the breadth of the wording of the money-laundering offence, it is difficult to envisage conduct involving the use of goods of unlawful origin which does not already in itself constitute the offence referred to in Article 648-*bis* of the Criminal Code.

Self-laundering (Art. 648-*ter*.1 of the Criminal Code) The offence of self-laundering punishes "anyone who, having committed or been an accomplice in committing an intentional crime, substitutes, transfers or uses in economic or financial activities money, goods or other benefits deriving from the commission of that crime in such a way as concretely to hinder the identification of their criminal origin". The penalty provided for is imprisonment from 2 to 8 years and a fine of between EUR 5,000 and EUR 25,000. The penalty is reduced to imprisonment from 1 to 4 years where the predicate offence underlying the laundering conduct carries a maximum term of imprisonment of less than 5 years.

The penalty is increased where the acts are committed in the exercise of a banking, financial or other professional activity; it is instead reduced if the person has taken steps to "prevent the conduct from being carried to further consequences or to secure evidence of the offence and the identification of the goods, money and other benefits deriving from the crime".

Self-laundering conduct is not punishable "where the money, goods or other benefits are allocated to personal use or enjoyment", provided that there was no intention thereby to conceal the proceeds of the offence.

The rules on self-laundering do not apply to persons who adhere to the "voluntary disclosure" procedure, that is, who cooperate voluntarily in the repatriation of capital unlawfully held abroad.

2. Purpose of this special part

This special part relates to conduct engaged in by the Corporate Bodies, Employees and Consultants, as further defined in the general part, involved in the category of sensitive activity.

The objective of this special part is to ensure that the persons identified above maintain conduct in compliance with the reference principles set out below, in order to prevent the commission of the offence indicated in the preceding paragraph.

The general part sets out the principles underlying the legislation and the principal safeguards for the implementation of the provisions in force in this area.

This special part identifies the reference principles for the construction of the Model, specifically provided for in relation to the category of sensitive activity identified, in order to prevent the commission of the offence of "self-laundering".

3. General reference principles

In carrying out all operations directly or indirectly connected with matters relating to the offence of "self-laundering", Employees and Corporate Bodies must adopt and comply with:

- the internal control system, and therefore corporate procedures, documentation and provisions relating to the corporate hierarchical/functional and organisational structure;
- the disciplinary system;
- generally, the applicable legislation.

4. General principles of conduct

This special part provides for an express prohibition binding on the Corporate Bodies (directly) and on the employees of Tagetik Software (limited, respectively, to the obligations contemplated in the specific procedures and to the obligations contemplated in the specific contractual clauses) on:

- engaging in, collaborating in or giving rise to the commission of conduct such that, considered individually or collectively, it constitutes, directly or indirectly, the category of offence referred to in Article 25-*octies* of Legislative Decree 231/2001 (self-laundering);
- breaching the corporate principles and procedures applicable to this special part.

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

The sensitive activities identified, with reference to the offence of self-laundering referred to in Article 25-*octies* of Legislative Decree 231/2001, are the following:

- MANAGEMENT OF CORPORATE OBLIGATIONS AND TRANSACTIONS
- MANAGEMENT OF ADMINISTRATIVE AND ACCOUNTING PROCESSES AND FINANCIAL FLOWS

With reference to the category of self-laundering, it should be borne in mind that, in addition to the activities listed above, self-laundering could also arise as a consequence of other non-negligent predicate offences under Legislative Decree 231/01 (by way of example only, consider bribery, fraud against the State, commercial fraud, offences against intellectual and industrial property, computer crimes, etc.), the proceeds of which could be the subject of "self-laundering" in the case of conduct aimed at concretely hindering the identification of their criminal origin.

6. General control principles

The general control principles underlying the tools and methodologies used to structure the specific control safeguards may be summarised as follows:

- **SEGREGATION OF DUTIES:** the application of the principle of separation of activities between those who authorise, those who execute and those who control is required;
- **EXISTENCE OF PROCEDURES/RULES/CIRCULARS:** there must be corporate provisions and formalised procedures capable of providing principles of conduct, operating methods for carrying out sensitive activities as well as methods for filing the relevant documentation;
- **AUTHORISATION AND SIGNATURE POWERS:** authorisation and signature powers must: i) be consistent with the organisational and managerial responsibilities assigned,

providing, where required, for the indication of expenditure approval thresholds; ii) be clearly defined and known within the Company;

- **TRACEABILITY:** every transaction relating to the sensitive activity must be adequately recorded. The process of deciding, authorising and carrying out the sensitive activity must be verifiable *ex post*, including by means of appropriate supporting documentation and, in any event, the cases and methods of any possible deletion or destruction of the records made must be regulated in detail.

7. Management of corporate obligations and transactions

The regulation of the activity must provide for what is established in detail by the reference Principles relating to the regulation of the sensitive activities "Transactions relating to share capital: management of contributions, corporate assets, profits and reserves, transactions involving shareholdings and capital" and "Management of financial flows".

8. Management of administrative and accounting processes and financial flows

The regulation of the activity must provide for what is established in detail by the reference Principles relating to the regulation of the sensitive activities "Preparation of financial statements, reports and corporate communications generally", as well as "Management of financial flows".

9. Controls by the Supervisory Body

Without prejudice to the discretionary power to take action through specific controls following reports received, the Supervisory Body does not carry out periodic controls of the activities of Tagetik Software S.r.l. potentially at risk of commission of the offences, in view of the risk assessment assigned when the Model was prepared and in the course of its subsequent updates.

It is nonetheless reaffirmed that the Supervisory Body is guaranteed free access to all relevant corporate documentation relating to the categories of Sensitive Activities.

A summary information flow must be addressed to the Supervisory Body whenever a transaction is carried out which, by reason of its characteristics, size or non-ordinary nature in relation to normal corporate operations, may relate to the matters dealt with in this chapter, such as, for example:

- extraordinary corporate transactions;
- the activation of financing by shareholders or third parties of a non-banking nature, or intercompany financing;
- capital transactions (e.g. capital increases, including by way of contributions);
- other extraordinary transactions or financial flows;
- investment transactions of particular significance.

10. Reference internal procedures and documents

The following internal procedures and documents are of reference for this special part:

1. Code of Ethics

2. Annual Financial Statements Preparation Procedure
3. Payments and Expense Reimbursements Procedure
4. IT Purchasing Procedure
5. Marketing Purchasing Procedure
6. Goods and Services Purchasing Procedure

These procedures and documents are to be regarded as supplementing and explaining the practices defined in this Special Part.

SPECIAL PART "G" — Employment of third-country nationals whose stay is irregular

1. The offences referred to in Article 22, paragraph 12 of Legislative Decree 286/1998 (Art. 25-*duodecies* of the Decree)

Legislative Decree 109/2012 expanded the catalogue of offences provided for by Legislative Decree 231/01: Article 25-*duodecies*, establishing as an offence "the employment of third-country nationals whose stay is irregular".

That offence occurs where the employer employs foreign workers who do not hold the residence permit provided for by Article 22 of Legislative Decree 286/98, or whose permit has expired and renewal of which has not been applied for within the statutory time limits, or has been revoked or annulled.

Article 25-*duodecies* extends the application of the decree to undertakings which have made use of foreign workers without a residence permit or with an expired permit, exceeding the limits laid down by Legislative Decree No. 286/1998, the "Consolidated Immigration Act", in terms of:

1. number of workers;
2. age;
3. working conditions.

Legislative Decree No. 109/2012 provides that the penalties governed by Article 22, paragraph 12 of Legislative Decree No. 286 of 25 July 1998, which states: "…An employer who employs foreign workers who do not hold the residence permit provided for by this article, or whose permit has expired and renewal of which has not been applied for within the statutory time limits, or has been revoked or annulled, shall be punished with imprisonment from six months to three years and a fine of EUR 5,000 for each worker employed".

Legislative Decree No. 109/2012 (published in Official Gazette No. 172 of 25 July 2012) inserted into Legislative Decree 231/01 Article 25-*duodecies*, "Employment of third-country nationals whose stay is irregular", with the following operative text:

"1. In relation to the commission of the offence referred to in Article 22, paragraph 12-*bis*, of Legislative Decree No. 286 of 25 July 1998, the entity shall be subject to a monetary penalty of between 100 and 200 units, up to a limit of EUR 150,000."

2. Risk areas

TAGETIK SOFTWARE S.R.L. is a company which punctually applies every statutory provision in employment matters; nonetheless, a risk profile has been considered in relation to Article 25-*duodecies*, given the significant internationalisation of the company, which controls various companies in third countries, and the consequent not insignificant presence of personnel working on secondment and/or coming from different countries and nationalities.

3. General rules of conduct

As a general rule, it is clearly prohibited to employ personnel from third countries who are not in compliance with the provisions of Legislative Decree 286/1998.

Consequently, all personnel who are hired by or in any event collaborate with Tagetik Software S.r.l. and who come from third countries but are domiciled, including temporarily, in Italy with a residence permit subject to expiry, must deliver to the Human Resources Office a copy of their valid residence permit both upon recruitment and/or at the start of the collaboration and upon each subsequent renewal.

The Human Resources Office must periodically verify that all personnel holding a residence permit subject to expiry are in compliance with the provisions of Legislative Decree 286/1998.

4. Reference internal procedures and documents

The following internal procedures and documents are of reference for this special part:

1. Code of Ethics
2. HR Procedure

These procedures and documents are to be regarded as supplementing and explaining the practices defined in this Special Part.

SPECIAL PART "H" — Tax offences

1. Tax offences (Art. 25-*quinquiesdecies* of the Decree)

The 2020 Tax Decree (Decree-Law 124 of 26 October 2019, converted into law by Law No. 157 of 19 December 2019) expanded the catalogue of offences provided for by Legislative Decree 231/01: Article 25-*quinquiesdecies*, inserting "tax offences" among the offences sanctionable under Legislative Decree 231/01.

The categories of offence provided for are the following:

Fraudulent tax return by means of invoices or other documents for non-existent transactions (Art. 2 of Legislative Decree No. 74/2000) The offence arises where a person, in order to evade value added tax or income tax, indicates fictitious cost items in the annual returns, making use of invoices or other documents for non-existent transactions. The crime is committed

where the person records the invoices in the accounting records or in any event holds them for evidentiary purposes vis-à-vis the tax authorities. In any event, the offence cannot be considered to have been committed until such elements are indicated in the annual return. It should be specified that the definition of "invoices or other documents" includes any document by which the person may prove the existence of deductible costs or deductible taxes.

Fraudulent tax return by means of other artifices (Art. 3 of Legislative Decree No. 74/2000) The crime is committed by a person who, in order to evade value added tax or income tax, indicates fictitious cost items or indicates revenue items lower than the actual ones in the annual returns, on the basis of a false representation in the accounting records and making use of fraudulent means capable of hindering assessment.

The thresholds of criminal liability which must be exceeded cumulatively are currently the following: - the amount evaded must exceed (per individual tax) EUR 30,000.00; - the revenue items withheld from taxation and the fictitious cost items must exceed 5% of the revenue items declared or, in any event, EUR 1,000,000.00.

The necessary elements of this offence are: a. the inaccuracy of the return deriving from the indication of revenue items lower than the actual ones or of fictitious cost items; b. the presence of a false entry in the accounting records; c. the use of fraudulent means, which must be other than false invoices, failing which the offence falls under fraudulent tax return by means of false invoices.

Issuing invoices or other documents for non-existent transactions (Art. 8 of Legislative Decree No. 74/2000) The offence arises where a person, in order to enable third parties to evade value added tax or income tax, issues invoices or other documents for non-existent transactions. The issuing and delivery of several invoices or other documents for non-existent transactions relating to the same tax period is regarded as a single offence. For the purposes of the moment of commission of the crime, what is relevant is the recording in the tax return of the document issued by the person who received it.

Concealment or destruction of accounting records (Art. 10 of Legislative Decree No. 74/2000) This offence punishes conduct involving the destruction or concealment of accounting records, the keeping of which is required by law, in order to prevent the reconstruction of the accounts by the competent authorities; for that reason, the offence may be committed only by those who are required to keep the accounts. For liability to arise, specific intent is required, that is to say the offender must have the specific purpose of evading income tax or value added tax or of enabling third parties to evade those taxes. No threshold of liability need be exceeded for the offence to be committed.

Fraudulent avoidance of payment of taxes (Art. 11 of Legislative Decree No. 74/2000) The offence of fraudulent avoidance of payment of taxes is committed by a person who, in order to avoid paying income tax or value added tax or interest or administrative penalties relating to those taxes amounting in total to more than fifty thousand euro, fraudulently disposes of assets or carries out other fraudulent acts in respect of their own or others' assets capable of rendering the enforced recovery procedure wholly or partly ineffective. For the crime to exist, it being an offence of concrete danger, it is sufficient that there be a debt of not less than fifty thousand euro; it is not required that an enforced recovery procedure has been commenced, but that acts have been carried out aimed at frustrating the successful outcome of any enforced recovery.

Subsequently to Law No. 157 of 19 December 2019, Legislative Decree No. 75 of 14 July 2020, "Implementation of Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law", extended the list of tax offences to the following categories:

Inaccurate tax return (Art. 4 of Legislative Decree No. 74/2000) The inaccurate tax return is a tax offence, committed with specific intent, in matters of income tax and VAT. For the offence to arise, two conditions must be met cumulatively, namely: the tax evaded, with reference to the individual tax, must exceed EUR 150,000.00; the total of the revenue items not indicated in the return and/or the non-existent cost items must exceed 10% of the total revenue items indicated in the return, or, in any event, their amount must exceed EUR 3,000,000.00. In addition to the aforementioned thresholds of liability set out above, the legislator has identified certain grounds of non-liability in the following cases:

- breaches arising from the interpretation of rules, where these are objectively uncertain;
- breach of the rules on accrual accounting resulting from consistent accounting practices disclosed in the financial statements (intent being absent);
- estimated valuations, where the correct estimate does not differ by more than 10% from that made: the amount of such differences does not count towards the calculation of the tax evaded or of the items withheld from taxation for the purposes of the thresholds of liability.

Failure to file a tax return (Art. 5 of Legislative Decree No. 74/2000) Failure to file a tax return arises where a person, in order to evade income tax or value added tax, fails to file the income tax or VAT return although required to do so. The threshold of liability for the offence of failure to file a tax return is currently EUR 30,000.00.

Undue set-off (Art. 10-*quater* of Legislative Decree No. 74/2000) The offence arises where a person fails to pay the sums due, using non-existent or non-applicable tax credits by way of set-off. The offence is completed at the moment when the undue set-offs exceed EUR 50,000 in a tax period.

Addressees of this special part

In view of the purpose of the categories of offence under examination, the following must be regarded as addressees of this Special Part:

- the Board of Directors;
- the bodies entrusted with the statutory audit;
- the functions responsible for preparing the financial statements, including the company's fiscal and tax advisers;
- all persons who perform functions and hold roles in administrative matters, such as, in particular, the management of the revenue cycle and the issuing of sales invoices;
- the functions responsible for managing the expenditure cycle and, in particular, the receipt, verification and recording of supplier invoices for subsequent payment.

2. Purpose of this special part

This Special Part has the purpose of preventing the offences indicated above, through the provision of a series of internal organisational measures aimed at the periodic or specific verification of compliance with tax legislation.

3. Risk areas

TAGETIK SOFTWARE Srl is a company which applies every statutory provision in tax matters; nonetheless, a risk profile has in any event been considered, in relation to Article 25-*quinquiesdecies*, arising from possible erroneous accounting entries and/or balance-sheet valuations which are significant for the purposes of the calculation and consequent payment of taxes.

In addition, any activities involving the removal/destruction of documents valid for tax purposes, including the management of documents retained electronically by way of substitutive archiving, are considered at-risk operations.

4. General rules of conduct

In carrying out administrative management activities, the procedures put in place to control the company's revenue and expenditure cycles must be complied with, as well as the procedure for the preparation of the annual financial statements and the mandatory legislation in this area.

It is therefore necessary to:

- comply with what is expressly provided for by the Company's Code of Ethics in matters of transparency, relations with corporate bodies and compliance with the law;
- know and apply the provisions of tax rules, including by requesting specific advice or support in this area;
- punctually comply with the requirements of internal procedures and corporate contracts as regards:
  - the issuing of sales invoices;
  - the verification, authorisation, recording and payment of supplier invoices;
  - the preparation of the annual financial statements;
  - the disposal of obsolete documents;
- exercise the utmost care in every accounting recording activity potentially capable of creating erroneous balance-sheet entries and/or of breaching the mandatory legislation in this area;
- exercise the utmost care in complying with statutory legislation in any activity involving the disposal of obsolete documents (whether paper-based or electronic) valid for tax purposes.

5. Controls by the Supervisory Body

In order to monitor compliance with the procedures and measures designed to avoid, as far as possible, breaches, including incidental ones, of the rules relating to tax offences, specific internal

verification audits must be carried out, on a planned basis, with and/or without prior notice, by the Supervisory Body and/or by its qualified appointees.

To that end, it is reaffirmed that the Supervisory Body and any appointees of the Supervisory Body are guaranteed free access to all relevant corporate documentation relating to the categories of sensitive activities.

6. Reference internal procedures and documents

The following internal procedures and documents are of reference for this special part:

- Code of Ethics
- Sales Invoice Issuing Procedure
- Payments and Expense Reimbursements Procedure
- Financial Statements Preparation Procedure

These procedures and documents are to be regarded as supplementing and explaining the practices defined in this Special Part.