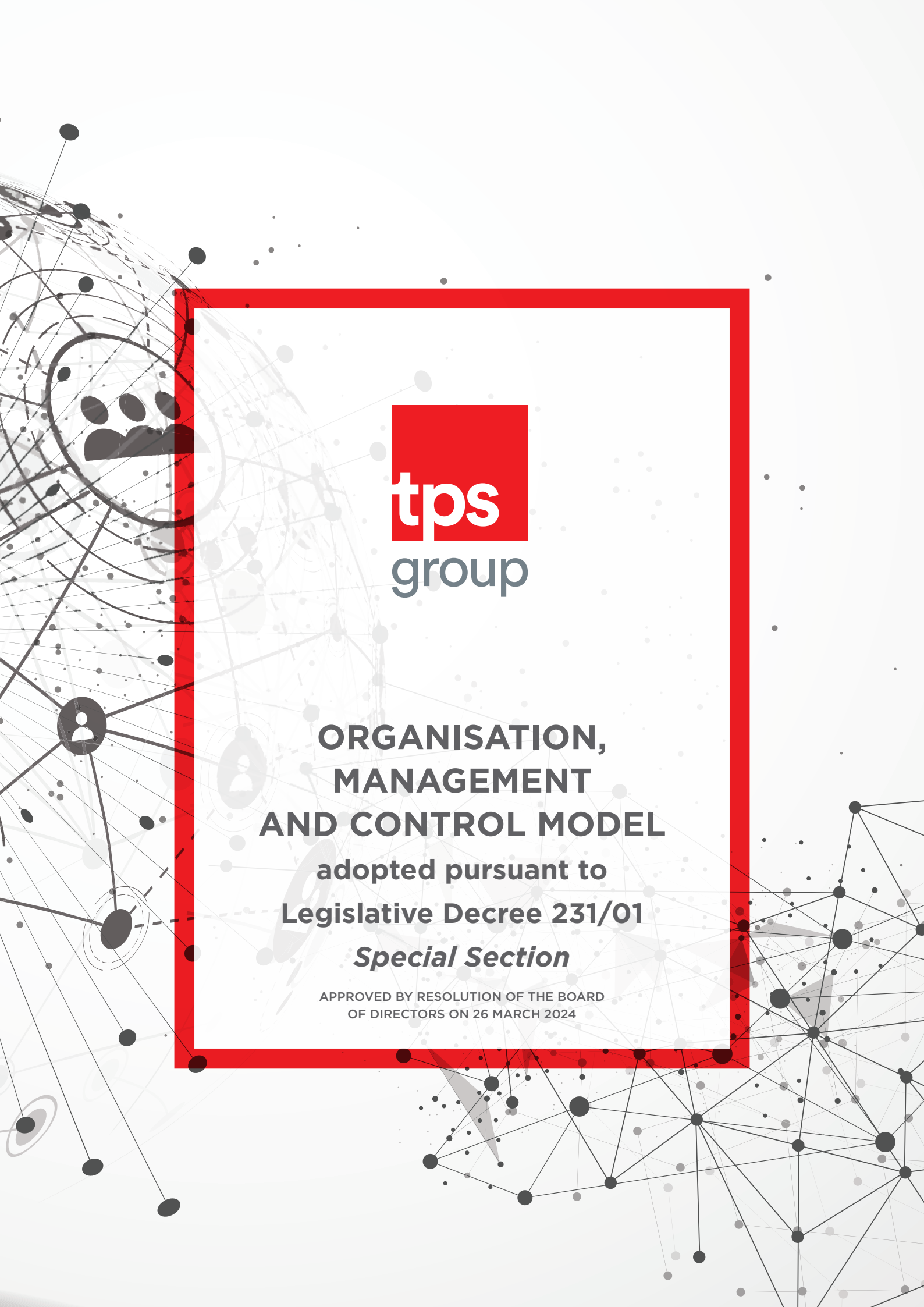

tps group

ORGANISATION, MANAGEMENT AND CONTROL MODEL

adopted pursuant to Legislative Decree 231/01

Special Section

APPROVED BY RESOLUTION OF THE BOARD
OF DIRECTORS ON 26 MARCH 2024

Contents

1. Revision

Rev.	Date	Comment	Approval
00	17 September 2019	First issue	Board of Directors
01	02 November 2020	Update for regulatory compliance	Chairman of the Board of Directors
02	26 March 2024	Second issue: adaptation to Legislative Decree 24/2023	Board of Directors

A. Offences in relations with the State, public bodies and the European Union
(Articles 24 and 25 of Legislative Decree No. 231/2001)

1) Description of Offences against the State, Public Bodies and the European Union referred to in Legislative Decree no. 231/2001

The company T.P.S. S.p.A. (hereinafter referred to as "TPS") intends to ensure the best possible effectiveness of the Organisational Model with which it has been equipped (hereinafter referred to as the "Model") and therefore deems it appropriate to outline below, albeit in concise form, the content of the offences referred to in Legislative Decree no. 231/2001, the commission of which by persons qualified under Article 5 of the aforementioned Decree may entail the occurrence of administrative/criminal liability for TPS.

The introductory paragraph of this chapter, in which a brief description of offences against the State, Public Bodies and the European Union is indicated, in order to make them known to all recipients, determines the model that has also been followed for the chapters devoted to the other offences covered by the Decree, which will be examined later.

That being said, the criminal offences referred to in Articles 24 and 25 of Legislative Decree no. 231/2001 establish the prohibition to engage in the conduct described below:

- Article 316-bis of the Criminal Code, misappropriation to the detriment of the State, a Public Entity or the European Union, an offence that may be committed by anyone outside the Public Administration who, having obtained from the State, a Public Entity or the European Union contributions, subsidies or funding intended to favour initiatives aimed at carrying out works or activities in the public interest, does not allocate them for the aforementioned purposes;
- Article 316-ter of the Criminal Code, undue receipt of disbursements to the detriment of the State, a public body or the European Union, an offence that may be committed by anyone, unless the act constitutes the offence specified in Article 640-bis of the Criminal Code, through the use or presentation of false declarations or documents or certifying untrue things, or through the omission of due information, unduly obtains, for himself/herself or for others, contributions, financing, subsidised loans or other disbursements of the same type, however denominated, granted or disbursed by the State, a Public Entity or the European Union;
- Article 353 of the Criminal Code, disturbance of public tenders, an offence that may be committed by anyone who, by means of violence or threats, or by gifts, promises, collusion or other fraudulent means, prevents or disrupts tenders in public tenders or private tenders on behalf of public administrations, or drives away the bidders.

- Article 353-bis of the Criminal Code, disturbance of the procedure for the choice of contractor, an offence that may be committed by anyone who, unless the fact constitutes a more serious offence, by means of violence or threats, or with gifts, promises, collusion or other fraudulent means, disturbs the administrative procedure aimed at establishing the content of the call for tenders or other equivalent act in order to condition the manner in which the public administration chooses the contractor.
- Article 356 of the Criminal Code, fraud in public supply, an offence that may be committed by anyone who uses deception to deceive the state, public or European Union counterparty or who, in simple contractual bad faith, maliciously alters the performance of the contract to the detriment of the state, public or European Union counterparty;
- Article 640, par. 2 (1) of the Criminal Code, fraud to the detriment of the State, a public body or the European Union, an offence that may be committed by anyone who, by artifice and deception, misleading someone, procures for himself or others an unjust profit to the detriment of others when the act is committed to the detriment of the State, a public body or the European Union;
- Article 640-bis of the Criminal Code, aggravated fraud to obtain funds from the State, a public body or the European Union, an offence which occurs if the act referred to in Article 640 of the Criminal Code relates to contributions, financing, subsidised loans or other funds of the same type, however denominated, granted or disbursed by the State, a public body or the European Union;
- Article 640-ter of the Criminal Code, computer fraud committed to the detriment of the State, a public body or the European Union, an offence which may be committed by anyone who, by altering in any way the operation of a computer or telecommunications system or by intervening without having the right to do so (par. 615-ter) in any way on data, information or programmes contained in a computer or telecommunications system or pertaining to it, procures for himself or others an unjust profit to the detriment of others, if one of the circumstances specified in paragraph 2 no. 1 of Article 640 of the Criminal Code applies;
- Article 318 of the Criminal Code, bribery for an act of office, an offence that may be committed by a public official who, in order to perform an act of his/her office, receives, for himself/herself or a third party, in money or other benefits, remuneration that is not due to him/her, or accepts the promise of such remuneration;
- Article 321 of the Criminal Code, penalties for the corruptor, which provides for the application of the penalties specified in Articles 318 to 320 of the Criminal Code also to a person who gives or promises the public official or the person in charge of a public service money or other benefits;
- Article 322 of the Criminal Code, incitement to bribery, an offence that can be committed by anyone and which is committed if the offer or promise is made in order to induce a public official or a person in charge of a public service to omit or delay an act of his/her office, or to perform an act contrary to his/her duties, if the offer or promise is not accepted;
- Article 319 of the Criminal Code, bribery for an act contrary to the duties of office, an offence that may be committed by a public official who, in order to omit or delay or to have omitted or delayed an act of his/her office, or in order to perform or to have performed an act contrary to the duties of office, receives, for himself/herself or for a third party, money or other benefits, or accepts the promise thereof;

- Article 319-ter of the Criminal Code, bribery in judicial proceedings, an offence that may occur when the acts referred to in Articles 318 and 319 are committed to favour or damage a party in civil, criminal or administrative proceedings;
- Article 319-quater of the Criminal Code, undue inducement to give or promise benefits, an offence committed by a public official or a person in charge of a public service who, abusing his/her position or powers, induces someone to give or promise unduly, to him/her or to a third party, money or other benefits;
- Article 317 of the Criminal Code, extortion, an offence that may be committed by a public official or a person in charge of a public service, who, abusing his/her position or powers, forces or induces someone to give or promise unduly, to him/her or to a third party, money or other benefits. Therefore, the relevant hypothesis for the activities carried out in concrete terms by TPS and for the qualification of the persons working at the Company is that of participation in the offence;
- Article 320-bis of the Criminal Code, bribery of a person in charge of a public service, which extends the application of Articles 319 and 318 to the public official as well as to the person in charge of a public service;
- Article 322-bis of the Criminal Code, embezzlement, extortion, bribery and incitement to bribery of members of the European Communities, by which it is provided that the provisions of Articles 314, 316, 317 to 320 and 311, third and fourth paragraphs, shall also apply to members of the Commission of the European Communities, the European Parliament, the Court of Justice and the Court of Auditors of the European Communities, in addition to other persons specifically identified by the provision and having employment relationships or belonging to bodies established on the basis of the Treaties establishing the European Communities.

The offences considered above presuppose the establishment and maintenance of relations with the State, Public Bodies and the European Union, therefore the persons at risk of the commission of one of the offences under consideration are essentially those who hold administrative and/or representative roles in TPS, who have the power to commit the Company towards third parties.

2) Identification of risk areas, sensitive processes and persons involved

Article 6(2)(a) of Legislative Decree No. 231/2001 provides that the Company must proceed to identify the risk areas, i.e. to examine and describe those, among its activities, where there is a risk of committing one of the offences expressly referred to in the Decree.

This analysis constitutes one of the essential elements of the Organisational Model, so TPS first carried out an analysis of the risk areas in which the Company operates.

On the basis of the results obtained, TPS identified the activities within the scope of which the offences referred to in Articles 24 and 25 of Legislative Decree No. 231/2001 could abstractly take place, with the highest degree of risk, and then examined the company's processes to verify which ones are among the "sensitive" ones.

The *way of working* just described will be followed by TPS with regard to all the executive protocols of which this Model is composed, i.e. with regard to all the types of offences referred to in Legislative Decree no. 231/2001 for which there is a risk of commission by the persons referred to in the Decree.

That being said, to supplement and specify what is indicated in Article 4.5 of the General Section of the Model, the *sensitive activities / risk areas* identified for

offences against the Public Administration are as follows (sensitive activities, which are listed below with the identification number assigned to them in the document entitled Risk Assessment):

- 1.1 Managing relations with the Guardia di Finanza (Tax Police) and Agenzia delle Entrate (Revenue Agency) for tax inspections
- 1.2 Calculation of direct and indirect taxes
- 1.3 Tax compliance management: preparing and transmitting telematic data / tax returns to the tax registry, making the relevant payments and paying taxes (Chamber of Commerce, Guardia di Finanza, Revenue Agency)
- 1.4 Management of regulatory, administrative and corporate obligations (e.g. filing of powers of attorney, filing of balance sheets, etc.) with Chamber of Commerce, Revenue Agency, etc.
- 1.5 Management of receipts and payments (settlement of invoices, etc.)
- 1.6 Cash and treasury management (opening/closing of current accounts; recording of receipts and payments in the general accounts; reconciliation of bank statements and cash transactions; management of the registers of the various company cash desks, etc.)
- 1.7 Management, control and authorisation of advances and reimbursement of expenses to employees and consultants
- 1.8 Management of missions / travels
- 1.12 Management of investments, financing, guarantees and, in general, relations with credit institutions
- 1.16 Opening and managing employee master data (attendance system)
- 1.25 Management of representation expenses incurred (with PA representatives, with commercial companies or with associations or other non-profit bodies)
- 1.29 Management of fulfilments for obtaining tax benefits (i.e. tax credit, etc.)
- 2.1 Management of inspections by public labour supervisory authorities (National Institute for Social Security (INPS), Local Health Authority (ASL), Labour Inspectorate)
- 2.2 Management of relations with bodies (such as the Province, INPS, INAIL, Employment Centre, Provincial Labour Directorate) for fulfilments relating to personnel administration and management (recruitment/termination, reports on the disabled present in the company, etc.). In particular, management of labour obligations and preparation of Form 770, DM10, INAIL self-assessment and F24 for payment of social security contributions and sending declarations to public bodies
- 2.3 Litigation management, coordination of legal advisers, filing of documents
- 2.4 Process management of:

  a) personnel selection
  b) recruitment of employees
- 2.5 Training Management
- 2.6 Management of relations with public bodies in connection with extraordinary events relating to personnel (redundancies, mobility, etc.)
- 5.9 Delivery of training activities

- 8.1 Managing relations with certification bodies for obtaining, implementing and maintaining the relevant certificates
- 9.2 Verification and control activities on compliance with waste management permits
- 9.4 Waste Identification Forms (FIR) management activities (issue, compilation and registration, etc.)
- 9.5 Compiling and maintaining waste registers (e.g. loading and unloading register)
- 9.6 Compilation of the annual MUD (Modello Unico di Dichiarazione ambientale - Single Environmental Declaration Form) and updating of the corresponding electronic program
- 9.7 Managing Environmental Communications
- 9.9 Waste Handling and Storage Activities
- 9.10 Water Discharge Management
- 9.11 Sampling and analysis before unloading
- 9.14 Management of relations with public authorities (such as Local Health Authority, ARPA (Regional Environmental Protection Agency), Labour Inspectorate, Municipal Police, State Forestry Corps, Province, Guardia di Finanza), in relation to environmental inspections
- 10.1 Management of relations with public authorities (Local Health Authority, Labour Inspectorate) in relation to inspections in the field of safety and hygiene at work (Legislative Decree no. 81/2008)
- 10.2 Management of the fulfilments required by Legislative Decree no. 81/08 on occupational safety and accidents, with Local Health Authority, the National Institute for Occupational Accidents Insurance (INAIL) and the Labour Office
- 10.11 Collection, processing and submission to PA bodies of technical, economic and administrative documentation required to obtain certifications, licences, concessions and administrative measures for the exercise of company activities
- 11.1 Purchase, management and use of information system and software licences

In view of the above, the main sensitive processes identified within the above-mentioned risk areas are:

1. Management of public funding and/or contributions:

a participation in procedures for applying for public funding and/or grants and the preparation of documentation produced or kept in support of applications;
b the actual receipt, use and destination of the financing and/or public contribution;
c documentation and reporting to the funding body and/or public grant awarding body, concerning the activities actually carried out and the destination of the amounts achieved.

2. Management of procedures for obtaining administrative authorisations, permits and licences:

a the evaluation, preparation and submission of applications for the purpose of obtaining and/or renewing measures (e.g. building permits and other licences in general, or health or other administrative authorisations in general);
b the payment of fees and/or taxes to be paid when submitting the application;
c inspections and/or checks by the competent authorities on compliance with the prerequisites for issuing the authorisation and/or licence.

3. Management of visits, inspections and, in general, management of all inspection activities by public authorities:

- **a** in tax matters;
- **b** in tax and/or social security matters;
- **c** in the field of safety at work;
- **d** in urban planning and construction;
- **e** generally any other inspection activities by public authorities.

4. Litigation management:

- **a** relations of all kinds in judicial and extrajudicial litigation in the various fields of civil, criminal, administrative and tax law;
- **b** coordination and management of external lawyers and the activities delegated to them.

5. Management of social security and welfare obligations:

- **a** preparation of communications, submission of contribution declarations and payment of social security contributions;
- **b** communications to the competent bodies on accidents, occupational diseases, recruitment/termination of employment;
- **c** preparation and transmission to the competent bodies of the necessary documentation for the recruitment of personnel belonging to protected categories or whose recruitment is facilitated.

6. Managing relations with the tax authorities and other public supervisory and control bodies:

- **a** submission of declarations for payment of taxes

7. Management of Import/Export activities:

- **a** customs management, possibly also through inland customs after its establishment

8. Environment, health and safety:

- **a** management of environmental compliance and waste disposal activities;
- **b** management of occupational safety and hygiene requirements.

The persons who may potentially commit one of the offences examined in this section are all those who have the power to represent the Company or who in any case have the power to commit the Company to making disbursements, hiring employees or in any case granting benefits or services to third parties. More specifically, these are: members of the Board of Directors; Chief Executive Officier; General Manager; holders of proxies; persons delegated to have relations with the P.A.; Privacy Officer; Prevention and Protection Service Manager (RSPP); persons with access to the computer system.

The degree of likelihood that one of the aforementioned offences will be committed appears to be limited, especially in view of the fact that TPS's activity does not focus from a negotiating point of view on relations with the PA but is based on the sale of services to commercial companies, so that in the absence of contracts, concessions or supplies to public entities, the areas of risk are reduced. However, the risk still exists, given the relations that the Company inevitably maintains with the PA for the bureaucratic fulfilments to which it is called upon in the ordinary course of its business.

3) Behavioural rules

Each person who will be entrusted with the management, in whole or in part, of relations with the PA shall act in full compliance with the corporate procedures, in any case basing his/her actions on the principles of fairness and transparency and complying with all the information obligations established in favour of the administrative bodies of the Company and the Supervisory Board.

For this purpose, it will be the responsibility of each person to have the documentation relating to each transaction, including non-economic transactions, performed within the scope of the assigned tasks and functions, made available and accessible.

In any case, it is strictly forbidden to engage in or collaborate in conduct that may directly or indirectly constitute the offences described above and referred to in Articles 24 and 25 of Legislative Decree No. 231/2001, it being understood that any violation of the rules contained in the procedures, in the Code of Ethics and, in general, in the documentation adopted in implementation of the reference principles specified in this Special Section is prohibited.

The management of dossiers as well as of contributions and/or financing of which the Company is a beneficiary and which may be available to it is exercised by the Administrative Manager on the basis of the power vested in him/her.

In addition to the above, the Company expressly forbids the following:

- **a** directly dispose of or make cash donations or in any case recognise other benefits in favour of public and non-public employees (including Italian or foreign Public Officials and Officials belonging to other public bodies under international law);
- **b** distribute free gifts and presents outside the scope of normal business practice or courtesy, or in any case, direct them to the beneficiary in order to acquire undue advantages or favourable treatment not due to the Company's business.
  The gifts that TPS may dispose of in favour of any beneficiary shall always be characterised by the smallness of their value, except in the case of donations in favour of social, cultural, artistic or ethical initiatives.
  The decision to offer gifts or donations outside the scope of normal business practice or courtesy must be adequately documented to allow the prescribed checks to be carried out, and must be formally taken by the management bodies, after informing the Supervisory Board;
- **c** perform services on behalf of agents, business associates, consultants and suppliers or pay them remuneration that is not adequately justified in the context of the contractual relationship existing with them or that is not adequately justified in the task entrusted to them;
- **d** use their position or influence in an instrumental manner in order to obtain benefits or privileges for themselves or others;
- **e** form and submit untruthful declarations or omit to communicate information to national or EU public bodies in order to obtain unjustified advantages or to obtain public grants, contributions or subsidised loans from the public authorities, the European Union or other public bodies under international law;
- **f** allocate public disbursements, contributions or subsidised loans received for purposes other than those for which they were intended;
- **g** circumvent and evade the prohibitions specified in points a), b), c) and f) through the payment or receipt of sums for any reason whatsoever (e.g. sponsorships) aimed at violating the obligations described and prohibited above.

The persons in charge of operating through the use of *personal computers* or computer systems of the Company are adequately trained and informed also with reference to the contents of Legislative Decree no. 196/2003 and Regulation (EU) 2016/679 (GDPR) on security, confidentiality and protection of personal data, as well as the procedures adopted by the Company and certified *ISO 27001*.

In any case, reference should be made to the provisions specified below devoted to the specific profile of computer offences, in which the use of personal computers, mobile telephony equipment and computer systems is regulated and the rules to be observed are described, provisions that are also useful for the prevention of the offences under consideration here, which are allegedly committed against the Public Administration through electronic means.

It is established that all recipients of the Model have a duty to refrain from providing or promising utilities, gifts or presents of significant value, or in any case disproportionate to the mere gifts that may be given to partners or employees on holidays.

4) Control Principles

TPS, in order to properly monitor the sensitive processes already mentioned, has defined the following specific rules and procedures (safeguards):

1. TPS has first of all established its organisation chart and job description ("Organisation chart", which is part of the Quality Manual established pursuant to the *"AS9100D / EN 9100:2018"* standard and published on its institutional portal *"People"*, which also contains all the operating procedures relating to the various company processes that will be mentioned later) so that:

- **a** the division of tasks and responsibilities is clearly defined, with the aim of separating as far as possible those who make or implement decisions, those who must give accounting evidence of the operations decided upon, and those who are required to carry out controls;
- **b** internal control mechanisms with binding force are in place, identifying systems for authorising, verifying and documenting significant decisions;
- **c** any power void or overlapping of roles and competencies is avoided.

For this purpose, the Company has adopted a system of proxies characterised by elements of certainty, such as to guarantee a clear and transparent representation of the internal procedures through which decisions are formed and implemented, requirements identified as necessary prerequisites for the achievement of an efficient management of the Company's business.

All persons who, on behalf of TPS, have relations with the P.A. and have the power to commit the Company externally must have a formal proxy specifying the powers conferred.

When certain persons, due to the function they hold within the Company and for the performance of the tasks assigned to them, must be vested with powers of representation, they shall be granted special powers of attorney of adequate content and suitable for the correct and effective performance of the functions, with specific and unequivocal definition of the powers of the delegate and specification of the limits of the power of attorney.

Each delegation must define exactly what powers the delegate may have, always bearing in mind that the powers assigned and their concrete exercise must not be in conflict with the Company's objectives and policies, and the delegate must have

the power to commit the Company and spend money in such a way that he/she can concretely perform the functions entrusted to him/her.

Powers of attorney shall also define the person to whom the delegate is required to report the results of his/her activities, while powers of attorney shall clarify, where provided for, any cases of revocation.

The Company has adopted appropriate organisational tools (such as organisational communications, procedures, etc.) with which it has provided for the description of roles and duties and described the tasks, powers and responsibilities assigned to each function. It then took steps to establish reporting lines within the Company, so that the formation of decisions and their implementation can be reconstructed through the traceability of the relevant steps of the process in function of the knowledge, transparency and publicity of the concrete exercise of the powers attributed.

TPS has instituted a separation, within each decision-making or operational process, between the person who makes the decision, the person who executes it and the person who is to carry out the controls on it, in order to ensure that the Company's activities are modelled on the principle of segregation of duties.

2. Another safeguard to protect the proper management of the Company, aimed at preventing the commission of offences, which may include offences against the PA, is the preservation and archiving of documents relating to business activities in such a way as not to allow their removal, alteration or subsequent modification, except with appropriate evidence

   The Company has adopted the rule by virtue of which access to archived documents may only take place by the person delegated to that specific ongoing relationship, specifically following a reasoned request, and is only allowed to the competent persons on the basis of the organisational chart and job description.

3. TPS, with regard to the third party collaborators it uses, establishes the prohibition of paying any remuneration, commission or commission to any consultant, collaborator, intermediary or public subject for amounts that do not correspond to the services rendered in its favour and that do not comply with the assignment conferred.

   The assessment must be carried out on the basis of reasonableness criteria and by reference to market conditions or practices or, to the extent that they have been repealed by recent regulatory measures, on the basis of the fee schedules of certain professional categories, which in any event constitute a reference indicator, taken as valid until such time as supplementary provisions replacing them are issued.

   The choice of external consultants to be engaged is always made on the basis of requirements of professionalism, competence and independence of the consultant or collaborator, and always with an expression of the reasons for the choice.

   With regard to employees, TPS will only use rewarding means of remuneration that, in terms of the size of the value of the rewards, are consistent with the work performed, the responsibilities entrusted and the results achieved, taking into account the employee's duties.

With regard to judicial, tax and administrative inspections, and therefore also to the management of relations with officials of social security and welfare institutions (INPS, INAIL, etc.) relating to labour relations, TPS establishes that only company officials expressly authorised to do so by specific delegation or by virtue of the

functions they hold must participate, without prejudice to the appropriateness of other persons being present on account of their knowledge of the sector or subject matter being inspected.

The Supervisory Board (hereinafter also referred to as the "SB") must be informed of each control or inspection activity by means of a specific communication and minutes must be drawn up of the entire inspection procedure, a copy of which shall be forwarded to the SB.

The administrative and accounting management system is structured to meet the criteria of transparency and traceability and is designed to allow all accounting data to be immediately detectable and controlled at all times. For this purpose, all administrative and accounting data of the Company are stored in an ERP system of appropriate standing, which TPS has identified as SAP.

If the Company should have to resort to complex procedures to obtain public financing of considerable amounts, the Board of Directors, through its bodies, may appoint, even from time to time, a Project Manager to whom the management of the procedure will be entrusted, with the obligation to proceed with periodic communication and reporting to the corporate governing bodies.

TPS also adopts precise control methods to prevent the presentation of data or false information aimed at unduly obtaining financing, funds or public funds for any reason whatsoever.

5) Specific protocols

To supplement the company's Code of Ethics and the principles listed above, TPS has adopted a number of specific protocols in order to raise the level of attention on activities at risk of commission of the offences referred to in Articles 24 and 25 of Legislative Decree No. 231/2001.

The protocols identified, whether provided for in the rules or formalised in specific company procedures or policies, are therefore intended to provide greater operational detail to the company functions operating in the processes and activities at risk of these offences being committed.

The Functions involved, the procedures and protocols adopted and the information flows to be forwarded to the Supervisory Board are summarised below.

Organis. Unit/Internal Manager	Documents /Procedures	Protocols	SB flows	Flow Periodicity
Head of the Department involved in the inspection		Sign the documents requested by the public administration during verification, only where authorised by appropriate proxy/ power of attorney Report in writing any critical issue and/or conflict of interest that may arise in the context of relations with the PA to the Head of General Management, the Chairman of the Board of Directors and/or the Board of Directors and the Supervisory Board	Reports on the following subjects: -list of visits, inspections and audits initiated or concluded during the reporting period, with an indication of the respective findings; - copies of the minutes of the inspections that were concluded with non-compliances and findings and sanctions imposed, if any.	Half-yearly
Head of Staff Management		Represent the company, to the extent of its competence and limited to the powers defined in the power of attorney by the Board of Directors, in civil, criminal, administrative and tax proceedings as well as before state, local and territorial tax offices. Handle the fulfilment of litigation (civil, criminal and administrative) with the competent judicial authorities, technical consultants and their auxiliaries and the management of regulatory fulfilments with municipalities, chambers of commerce and independent authorities	Reports on the following subjects: -list of ongoing proceedings; -list of out-of-court settlements (criminal, civil and administrative litigation) signed by the Company or in the process of being settled; -list of assignments given to lawyers and the progress of judicial and/or extrajudicial activities.	Half-yearly

B. Computer crimes and illicit data processing; Crimes relating to infringement of copyright

(Art. 24-Bis and Art. 25-Nonies of Legislative Decree no. 231/2001)

1) Identification of relevant conduct and risk areas in relation to computer crimes and unlawful processing of data

The criminal offences referred to in Article 24-bis of Legislative Decree no. 231/2001 establish the prohibition to engage in the conduct described below:

- 1. Forgery of a public computer document or one having evidentiary effect (Article 491-bis of the Criminal Code);
- 2. Unauthorised access to a computer or telecommunications system (Article 615-ter of the Criminal Code);
- 3. Unauthorised possession and distribution of access codes to computer or telematic systems (Article 615-quater of the Criminal Code);
- 4. Dissemination of computer equipment, devices or programs intended to damage or interrupt a computer or telecommunications system (Article 615- quinquies of the Criminal Code);
- 5. Unlawful interception, obstruction or interruption of computer or telematic communications (Article 617-quater of the Criminal Code);
- 6. Installation of equipment designed to intercept, prevent or interrupt computer or telematic communications (Article 617-quinquies of the Criminal Code);
- 7. Damage to computer information, data and software (Article 635-bis of the Criminal Code);
- 8. Damage to computer information, data and software used by the State or other public body or in any case of public utility (Article 635-ter of the Criminal Code);
- 9. Damage to computer or telecommunications systems (Article 635-quater of the Criminal Code);
- 10. Damage to computer or telecommunications systems of public utility (Article 635-quinquies of the Criminal Code);
- 11. Computer fraud by the electronic signature certifier (Article 640-quinquies of the Criminal Code).

The *areas of risk* in which the violation of the criminal provisions referred to in Legislative Decree No. 231/2001 could occur, with the consequent hypothetical contestation of liability against TPS, are the following:

- 1. areas in which the activities of the recipients of the Model involve the use of the Company's IT tools, electronic mail and access to the Internet;
- 2. areas relating to the management of the Company's computer network, with activities aimed at ensuring its operation, maintenance and development.

On this basis, the following sensitive *activities* have been identified (sensitive activities, which are listed below with the identification number assigned to them in the document entitled Risk Assessment):

- 1.27 Electronic invoicing
- 1.28 Back up with computer tools of the accounting archive
- 2.7 Managing confidential and sensitive employee data in paper and digital form
- 11.1 Purchase, management and use of information system and software licences
- 11.2 Maintenance of IT equipment
- 11.3 Definition and periodic management of backups, antivirus systems, firewalls and network protection, physical server and workstation security
- 11.4 Managing how internal and external users access systems
- 11.5 Access verification and tracking of data changes made by users
- 11.7 Privacy system management (management and verification of security measures for sensitive data, management of privacy mandates, management of authorisations for data processing by IT means, provision of training, etc.)
- 11.8 Management of confidential and sensitive data (e.g. employee and supplier data) in digital format
- 11.9 Management of the Company's website
- 11.10 Incident and IT security management

2) Copyright infringement offences, identification of relevant conduct, sensitive processes and persons involved

Article 25-nonies of Legislative Decree No. 231/2001 refers to the offences provided for in Articles 171, paragraph 1 a-bis), and paragraph 3 171-bis, 171-ter, 171-septies and 171-octies of Law No. 633 of 22 April 1941, or offences committed in breach of copyright.

The sensitive processes detected can be identified in all the activities carried out by TPS employees or collaborators that involve the use of the Company's computer systems, programmes or applications, with a slight deviation of risk in those areas in which the frequency, complexity and criticality of the use of computer systems is greater and in which the IT skills of the persons involved are higher.

On this basis, the following *sensitive activities* have been identified (which are listed below with the identification number assigned to them in the document entitled Risk Assessment):

- 5.1 Technical publications management (ATA/AER)
- 5.2 Electronic and mechanical design
- 5.3 Definition, development and integration of avionics processes
- 5.4 Electromechanical parts installation kit design
- 5.5 Technical Publications Management - Computer Based Tranining (CBT)
- 5.6 Technical Publications Management - ASD 1000D
- 5.7 Multimedia Content Management
- 5.8 Creation of augmented and virtual reality applications
- 11.1 Purchase, management and use of information system and software licences
- 11.2 Maintenance of IT equipment
- 11.6 Managing IT security aspects of electronic documents with evidentiary value
- 11.9 Management of the Company's website

In view of the activity carried out by TPS, the risk that one of the above-mentioned offences may be committed by any of the recipients of the Model and to the benefit of the Company appears to be limited, with reference to the conduct envisaged by Article 171-bis of Law No. 633 of 22.04.1941 (duplication of computer programs). In any case, for the sake of clarity, each person who is assigned company IT equipment is required to comply with the Policy in force on the subject, a copy of which is distributed to each employee and collaborator, who acknowledges receipt thereof, at the time of assignment.

The offences in question could abstractly be committed by anyone in the Company who employs computer systems connected to the Internet, or who in any case has access to third-party programmes without a suitable licence for the purpose of carrying out their activities.

3) Behavioural rules

Each individual user is informed, warned and made accountable by the Privacy Officer and the IT Department, so that data transmission, saving and storage activities used for service reasons always take place in compliance with the safeguards, procedures and rules specified by the Company to protect the security, integrity and confidentiality of data.

Specifically:

- 1. it is forbidden to use the Internet connection for reasons unrelated to one's professional activities, with an express prohibition, in particular, to connect to websites that may be considered unlawful in the light of the provisions of the internal organisational provisions in question (by way of example, sites that promote or support terrorist or subversive

movements, sites that may be linked to hacking activities, or sites that violate the rules established on copyright and intellectual property);

- 2. it is forbidden to violate, or even to attempt to violate, computer systems belonging to or containing data of competing companies in order to acquire commercial information that could benefit TPS or that could damage competitors, or in order to illegitimately obtain third-party documentation, just as it is strictly forbidden to damage the technological or computer tools of third parties or of competing companies in order to impede their regular activity or to damage their operation;
- 3. the Company establishes the prohibition for all the recipients of the Model, except for the person in charge of Privacy and the Information Technology Sector and the technicians in charge of operating or maintaining or repairing the information systems, and only for the performance of such operations, to install and use programs or software that are not envisaged or approved by the Company and that are not functional for the performance of the work to be carried out in the Company;
- 4. it is also established that it is absolutely forbidden to modify the configurations of the software and hardware set up by the Company, as well as to circumvent in any way the protection and security rules specified to protect the Company's IT tools or to modify in any way the configuration of the fixed or mobile workstations assigned by the Company;
- 5. it is forbidden to carry out computer access outside one's authorisation level;

4) Control Principles

In relation to the safeguards, TPS provides the recipients of the Model with adequate and continuous information on the correct use of the Company's IT tools and on the risks of commission of the offences specified in Articles 24-bis and 24-nonies of Legislative Decree No. 231/2001, so that everyone is aware of the updated content of the legislation applicable to the matter in question.

Further safeguards that TPS has adopted to prevent computer crimes and unlawful data processing are as follows:

- 1. TPS appoints an internal IT Manager with specific technical expertise, who is entrusted with the tasks of providing (or appointing persons to provide) the management and development of the infrastructure, as well as control activities relating to the use of IT systems by the persons authorised to use them;
- 2. the Company's computer system is equipped with software, firewalls and antivirus software suitable for preventing threats to the systems from damaging, in whole or in part, their components and contents, and TPS ensures that these protection systems are never disabled;
- 3. the company's computer network must be subject to regular and continuous checks in order to verify its efficiency and technical adequacy over time

with respect to the company's needs. This implies the obligation to take immediate action in the event of system failures, gaps or weaknesses, so as to promptly remedy them and to report inadequacies in the system to allow for their implementation, always keeping evidence of the checks carried out and all actions taken;

- 4. appropriate procedures are in place for authentication and subsequent access to IT tools, as well as for the assignment and management of usernames and passwords, with the setting of validity periods for them and the use of an automatic routine that monitors the password schedule and provides for their compulsory change every 40 days;
- 5. employees are notified or given access credentials to the TPS computer system by the Head of the Information Technology Department, and thus through the use of the credentials, to the data and information contained in the system, by means of personalised quota access;
- 6. with regard to credentials, granted within the limits in which access is necessary for the correct performance of the task, in line with the Company's objectives, all recipients of the Model are obliged not to disclose, hand over or in any case share with anyone, internal or external to the Company, any of the information relating to access to the Company's or third parties' systems and network;
- 7. each individual user must be informed and made responsible by the Head of the IT Department as to the function and manner of use (data are saved and stored on the server on a daily basis), with an awareness of the limits of use of the Company's IT and telematic tools, with particular reference to the Internet and e-mail, which may only be used for service reasons;
- 8. in the event of the use of wireless connection systems to connect to the Internet network, TPS adopts tools to protect its network through the provision of an access keyword, so that any third party, external to the Company, is prevented from being able to illicitly connect to the Internet network managed by the Company and engage in unlawful conduct that could be ascribed to employees;
- 9. in the event of connection to the Company's computer network from outside, the latter shall provide for access limitations through the provision, adoption and maintenance of authentication systems in addition to those set up for access by internal recipients, possibly providing not only a username and password but also an additional password or code necessary for access and use of the system.

5) Specific protocols

To supplement the company's Code of Ethics and the principles listed above, TPS has adopted a number of specific protocols in order to raise the level of attention on activities at risk of commission of the offences referred to in Articles 24-bis and 24-nonies of Legislative Decree No. 231/2001.

The protocols identified, whether provided for in the rules or formalised in specific company procedures or policies, are therefore intended to provide greater

operational detail to the company functions operating in the processes and activities at risk of these offences being committed.

The Functions involved, the procedures and protocols adopted and the information flows to be forwarded to the Supervisory Board are summarised below.

Organis. Unit/Internal Manager	Documents /Procedures	Protocols	SB flows	Flow Periodicity
IT infrastructure and software manager	Regulation on the use of company computer equipment ISO 27001 procedures	Ensure that only authorised and certified software is purchased and used Ensure that in order to install software other than that made available by the Company, prior authorisation must be obtained from the IT infrastructure and software manager	Reports on the following subjects: -up-to-date inventory of software in use by the Company and its licences; -copies of contracts governing relations with outsourcing service providers/IT consultants.	Yearly

C. Crimes of counterfeiting money, receiving stolen goods, money laundering, use of money, goods or benefits of unlawful origin

(Articles 25-bis and 25-octies of Legislative Decree no. 231/2001)

1) Identification of risk areas, sensitive processes and persons involved

The criminal offences referred to in Articles 25-bis and 25-octies of Legislative Decree no. 231/2001 prohibit the commission of the offences described below:

- 1. Counterfeiting, spending and introducing into the State, acting in concert, counterfeit money (Article 453 of the Criminal Code);
- 2. Alteration of currency (Article 454 of the Criminal Code);
- 3. Spending and introduction into the State, without acting in concert, of counterfeit money (Article 455 of the Criminal Code);
- 4. Spending of counterfeit money received in good faith (Article 458 of the Criminal Code);
- 5. Forgery of revenue stamps, introduction into the State, purchase, possession or putting into circulation of forged revenue stamps (Article 459 of the Criminal Code);
- 6. Counterfeiting watermarked paper in use for the manufacture of public credit cards or stamps (Article 460 of the Criminal Code);
- 7. Manufacture or possession of watermarks or instruments intended for the counterfeiting of money, revenue stamps or watermarked paper (Article 461 of the Criminal Code);
- 8. Use of counterfeit or altered stamps (Article 464 of the Criminal Code);
- 9. Counterfeiting, alteration or use of distinctive signs of original works or industrial products (Article 473 of the Criminal Code);
- 10. Fraudulent transfer of valuables (Article 512-bis of the Criminal Code),
- 11. Introduction into the State and trade of products with false signs (Article 474 of the Criminal Code).
- 12. Receiving stolen goods (Article 648 of the Criminal Code), Money laundering (Article 648-bis of the Criminal Code), Use of money, goods or benefits of unlawful origin (Article 648-ter of the Criminal Code) and Self laundering (Article 648-ter.1 of the Criminal Code).

In the context of the activities carried out by the Company, it can be considered that the risk of the above-mentioned offences being committed is very limited, because the Company habitually makes payments by means of bank transfers or remittances, whereas cash is not a widespread means of payment in the performance of business activities.

There is a petty cash box at the Company which is used to make small payments, mostly to employees who have to travel in the course of their work, but the amounts held and handled there are very small.

Having said this, the following sensitive *activities* have been identified (sensitive activities are listed below with the identification number assigned to them in the document entitled Risk Assessment):

- 1.5 Management of receipts and payments (settlement of invoices, etc.)
- 1.6 Cash and treasury management (opening/closing of current accounts; recording of receipts and payments in the general accounts; reconciliation of bank statements and cash transactions; management of the registers of the various company cash desks, etc.)
- 1.7 Management, control and authorisation of advances and reimbursement of expenses to employees and consultants
- 1.8 Management of missions / travels
- 1.12 Management of investments, financing, guarantees and, in general, relations with credit institutions
- 1.16 Opening and managing employee master data (attendance system)
- 1.18 Checking consistency between purchase invoice and prices, quantity and type of material received in stock
- 1.20 Customer and supplier master data management and maintenance
- 1.21 Recording of invoices (receivable and payable) and credit notes
- 1.23 Managing the accounting of advance payments to suppliers
- 1.25 Management of representation expenses incurred (with PA representatives, with commercial companies or with associations or other non-profit bodies)
- 3.1 Negotiation activities with customers
- 3.2 Determination of contractual conditions and price
- 3.3 Signing of contracts, commercial agreements, framework agreements
- 3.4 Management and maintenance of customer master data: data entry/ updating, commercial and professional customer verification
- 3.5 Management of activities related to the organisation of and/or participation in events for promotion purposes
- 3.6 Sponsorships
- 4.1 Planning of requirements and management of purchase requests for the supply of goods and services
- 4.2 Supplier evaluation, qualification and monitoring activities and annual qualification renewal
- 4.3 Contracting and signing purchase contracts with suppliers

- 4.4 Issuing, correcting and updating purchase orders
- 4.5 Awarding of professional and specialist consultancies
- 4.7 Verification of services received with regard to professional appointments and specialist advice to third parties
- 7.5 Workshop management tools and spare parts for maintenance activities
- 8.7 Support in supplier qualification activities and annual re-evaluation of suppliers
- 9.8 Waste management (hazardous/non-hazardous)

The persons who may in abstract terms give rise to the conduct under consideration are the members of the Board of Directors; Chief Executive Officer; General Manager, Administrative Director; Cash Handlers, Procurement Service.

2) Behavioural rules

In the performance of the corporate activities considered to be at risk, all direct recipients of the Model, including consultants and collaborators, must comply with the following general principles of conduct to be understood as additional safeguards for the prevention of the offences under consideration:

- 1. formulating a judgement with regard to the reliability of suppliers so as to be able to verify their reliability, correctness and to be able to analyse the traceability of economic transactions carried out with them, avoiding the creation or continuation and increase of business relations with parties that do not have, or are not able to maintain over time, the necessary requirements of transparency and correctness;
- 2. verify that suppliers or collaborators and consultants continue to meet the requirements of reliability, correctness, professionalism and honourableness that the Company considers essential for its business activities;
- 3. refrain from engaging in business or collaborative relations with persons who are known or even suspected to belong to criminal systems and organisations or, in any case, who operate outside the scope of regularity and full legitimacy, such as, for example, persons linked to money laundering, arms or drug trafficking, usury;
- 4. not use anonymous instruments to carry out transfer transactions of significant amounts;
- 5. set up and keep up-to-date the supplier database;
- 6. promptly report all transactions that may present risk or suspicion profiles, with reference to the legitimacy of the origin of the sums involved in the transaction or to the reliability and transparency of the supplier or collaborator;
- 7. prohibition of concealing the proceeds of any offence committed in the alleged interest or to the advantage of the Company

3) Control Principles

TPS is not included among those who are recipients of the obligations imposed by Legislative Decree no. 231/2007 (hereinafter also referred to as the "Anti-Money Laundering Decree"), but it is appropriate to take into account the possibility that the Company, like any other legal entity, may be charged with committing one of the Crimes covered by this section, through one of the conducts envisaged and punished by Articles 648, 648-bis, 648-ter and 648-ter.1 of the Criminal Code.

Hence the need to implement careful monitoring of activities, as follows :

- 1. formalise the contractual terms and conditions governing relations with suppliers and commercial and financial partners, including between companies belonging to the Group.
- 2. analysing and verifying that payments are executed in a regular manner, especially with regard to the coincidence between the recipients and/or originators of payments and the counterparties that are actually and formally involved in the transactions;
- 3. ensure transparency and traceability of financial transactions;
- 4. carry out checks and controls, both formal and substantive, on incoming and outgoing financial flows, with specific reference to payments made in favour of third parties, also taking into account both the registered office indicated by the company or by the supplier or collaborator, and the credit institutions designated for payments and then concretely used, also assessing the existence and structure of any corporate shields or the presence of trustee organisations used for extraordinary transactions or operations;
- 5. use or employ only economic and financial resources whose origin has been verified and only for transactions that have an express reason and are recorded and documented;
- 6. give concrete implementation to constant training and provide information to the recipients of the Model on issues relevant from time to time and related to the prevention and suppression of money laundering phenomena;
- 7. with regard to bribery offences, those deriving from tax evasion and/or the unlawful appropriation of corporate assets, offences from which statistically one of the forms of conduct punishable by the offence of self-laundering could more frequently be derived, the Company refers herein to the existing safeguards with reference to offences against the PA, corporate offences and those provided for by the Code of Ethics and the General Section of the Model concerning the use of corporate assets.

4) Specific protocols

To supplement the company's Code of Ethics and the principles listed above, TPS has adopted a number of specific protocols in order to raise the level of attention on activities at risk of commission of the offences referred to in Articles 25-bis and 25-octies of Legislative Decree No. 231/2001.

The protocols identified, whether provided for in the rules or formalised in specific company procedures or policies, are therefore intended to provide greater operational detail to the company functions operating in the processes and activities at risk of these offences being committed.

The Functions involved, the procedures and protocols adopted and the information flows to be forwarded to the Supervisory Board are summarised below.

Organis. Unit/Internal Manager	Documents /Procedures	Protocols	SB flows	Flow Periodicity
Head of Administration, Finance and Control	RPO600 - Finance Administration Management	In the event that the Company is proposed to undertake anomalous transactions, the transaction must be suspended and assessed in advance by the Administrative Body and the Supervisory Board, which shall express its opinion on the advisability of the transaction and, if necessary, provide for the necessary precautions to be taken for the continuation of negotiations, and shall render an opinion on the matter that shall be taken into account when approving the transaction	Reports on the following subjects: -list of abnormal transactions	Yearly

D. Corporate offences; market abuse
(Art. 25-Ter and Art. 25-Sexies of Legislative Decree no. 231/2001)

1) Description of the Corporate Crimes referred to in Legislative

Article 25-ter sub-paragraphs a) to s-ter) of Legislative Decree no. 231/2001 refers to a series of criminal offences, including those described below:

- false corporate communications (Articles 2621 of the Civil Code, 2621-bis of the Civil Code and 2622 of the Civil Code);
- impeded control, provided for in Article 2625 par. 2 of the Civil Code;
- fictitious capital formation, provided for in Article 2632 of the Civil Code;
- undue return of contributions, as provided for in Article 2626 of the Civil Code;
- illegal distribution of profits and reserves, provided for in Article 2627 of the Civil Code;
- Unlawful transactions involving shares or quotas of the company or its subsidiaries, as provided for in Article 2628 of the Civil Code;
- transactions to the detriment of creditors, provided for in Article 2629 of the Civil Code;
- fictitious capital formation, provided for in Article 2632 of the Civil Code
- undue distribution of company assets by liquidators, provided for in Article 2633 of the Civil Code;
- bribery among private individuals and incitement to bribery among private individuals as referred to in Articles 2635 par. 3 and 2635-bis of the Civil Code;
- unlawful influence on the assembly, provided for in Article 2636 of the Civil Code;
- failure to disclose a conflict of interest, as provided for in Article 2629-bis of the Civil Code;
- market rigging, provided for in Article 2637 of the Civil Code;
- obstructing the exercise of the functions of public supervisory authorities, provided for in Article 2638 par. 1 and par. 2 of the Civil Code.

TPS considers that there is a risk, to a greater or lesser degree, that the persons indicated in Article 5 par. 1 of the Decree may engage in conduct in violation of the above-mentioned rules, to which, therefore, particular attention was paid in the risk assessment activity and identification of risk areas and sensitive processes.

2) Description of the Offences of Market Abuse referred to by Legislative Decree No. 231/2001

Article 25-sexies of Legislative Decree No. 231/2001 refers to a series of criminal offences:

- Abuse of inside information (Article 184 CFA Legislative Decree no. 58 of 24.02.1998);
- Market manipulation (Art. 185 CFA) Legislative Decree no. 58 of 24.02.1998).

3) Identification of risk areas, sensitive processes and persons involved

TPS has preliminarily identified the risk areas, in which infringements of the aforementioned rules could occur, with the consequent configuration of the offences provided for in Articles 25-ter and 25-sexies of the Decree, *risk areas/ sensitive activities* which, at the outcome of the assessments, were respectively the following (sensitive activities which are listed below with the identification number attributed to them in the document entitled Risk Assessment)

For the Corporate Offences referred to in Article 25-ter of Legislative Decree No. 231/2001

- 1.2 Calculation of direct and indirect taxes
- 1.3 Tax compliance management: preparing and transmitting telematic data / tax returns to the tax registry, making the relevant payments and paying taxes (Chamber of Commerce, Guardia di Finanza, Revenue Agency)
- 1.7 Management, control and authorisation of advances and reimbursement of expenses to employees and consultants
- 1.8 Management of missions / travels
- 1.9 Valuations and estimates of subjective balance sheet items; recognition, recording and representation of business activities in accounting records, reports, financial statements and other business documents; updating the chart of accounts
- 1.10 Registration of extraordinary transactions (e.g. mergers, acquisitions, etc.)
- 1.11 Disposal of corporate real estate or participations
- 1.13 Preservation of documents over which other corporate bodies could exercise control (e.g. company books, accounting records, etc.)
- 1.14 Management of Relations with Shareholders and the Supervisory Board
- 1.17 Processing of pay slips, linking of accounting data and pay slips and accounting for labour costs
- 1.18 Checking consistency between purchase invoice and prices, quantity and type of material received in stock
- 1.19 Customer schedule of payments management
- 1.21 Recording of invoices (receivable and payable) and credit notes
- 1.22 Monitoring of invoices due to be received
- 1.23 Management of the accounting of advance payments to suppliers
- 1.24 Archiving of supporting documentation for invoices issued and received
- 1.25 Management of representation expenses incurred (with PA representatives, with commercial companies or with associations or other non-profit bodies)
- 1.26 Recording the loading and unloading of goods in the warehouse
- 1.27 Electronic invoicing
- 1.28 Back up with computer tools of the accounting archive
- 1.29 Management of fulfilments for obtaining tax benefits (i.e. tax credit, etc.)

- 1.30 Intra-group transactions
- 1.31 External Communication and Media Relations
- 2.5 Training Management
- 3.5 Management of activities related to the organisation of and/or participation in events for promotion purposes
- 3.6 Sponsorships
- 4.3 Contracting and signing purchase contracts with suppliers
- 4.4 Issuing, correcting and updating purchase orders
- 4.5 Awarding of professional and specialist consultancies
- 4.7 Verification of services received with regard to professional appointments and specialist advice to third parties
- 11.9 Management of the Company's website

The sensitive processes identified can be represented as follows:

a) entries, records and the general keeping of company and accounting books;
b) all accounting and valuation steps leading to the formation of the budget;
c) ordinary management of accounts;
d) current and repeated relations with the Board of Auditors and the Auditors;
e) the preparation of the data, documents and elements necessary for the preparation of corporate reports and to provide due information to the members;
f) preparation and implementation of the delegation system;
g) management of negotiation activities;
h) approval of the resolutions of the Board of Directors and their implementation by delegated persons in relation to ordinary and extraordinary transactions, share capital, management of contributions, distribution of profits and reserves and transactions on shareholdings;
i) constitution and functioning of assemblies;
j) external communications and media relations.

The persons who may abstractly commit the offences described above are first and foremost the members of the Board of Directors, the Chief Executive Officer, the General Manager, the Executives, the Administrative Manager, the Statutory Auditors, the Auditors and the Liquidators.

As a residual and abstract possibility, it is also possible to hypothesise the concurrent liability of other persons, including in particular those who assist in the preparation and drafting of the financial statements or those who are entrusted with the disclosure of data and information with a margin of discretion. These parties are in any case obliged to comply with the provisions herein.

In addition, the punishable persons, and thus the direct recipients of the provisions of this section, are also those third parties who, in the event of simulated or fraudulent acts and who alter the proceedings of the shareholders' meeting, thereby procuring an unfair profit for themselves or others, so that the legislature has introduced an amendment to the article on unlawful influence on the shareholders' meeting with reference precisely to active subjectivity, extending the punishability from shareholders alone to extraneous third parties acting on their proxy. The degree of risk referring to the possibility of commission of corporate offences appears to be low because the financial statements, a document for the

preparation and drafting of which some of the offences could occur more frequently, are prepared by the offices and persons identified as competent by corporate procedures and are submitted to the assessment of all the members of the Board of Directors, thus implementing a cross-assessment of what is specified therein.

The segregation of duties and delegation of powers provided for in the job description, the Code of Ethics and the controls of the Board of Auditors and the Auditing Firm constitute further safeguards put in place to prevent the occurrence of prohibited conduct that is harmful to third parties.

4) Behavioural rules

TPS requires all the recipients of the Model entrusted with or in any case involved in the activities aimed at preparing and drafting the financial statements, periodical accounting entries and other corporate communications, to behave correctly and transparently at all times, ensuring full compliance with all legal and regulatory provisions, as well as with all the Company's internal procedures, in order to provide shareholders, creditors and third parties with a clear and truthful representation of the Company's equity, economic and financial situation.

The recipients of the Model must always act in strict compliance with all the rules specified by law to protect the integrity of the share capital, so that the function of guaranteeing creditors and third parties, which is generally the function of capital, is not impaired.

It is forbidden to engage in simulated transactions or to disseminate false information or in any case information likely to cause an illegitimate and appreciable alteration in the price of financial instruments, while TPS is constantly committed to promptly, correctly and transparently make all the communications required by law, without hindering the exercise of supervisory functions by the competent Authorities.

The Company, in consideration of the sensitive processes identified, also expressly prohibits

- form, include, represent or in any case transmit in the financial statements, reports and prospectuses or in other corporate communications, or communicate them by means of the above-mentioned documents, data that are false, incomplete, do not correspond at least in part to reality, and in any case are likely to present an altered description of the company's equity, economic and financial situation;
- omit the communication of data and information whose transmission is required by law on the economic and financial situation of the Company;
- illustrate the data and information used for the valuations made by TPS in such a way as to provide a representation that does not correspond to the actual judgement matured on the company's equity, economic and financial situation and the evolution of its business;
- act in violation of the principle of reasonableness during the activities of estimating accounting items and concealing or not clarifying which valuation criteria were used as the basis for the estimates, without providing the necessary information to ensure the correctness and truthfulness of the documents;
- evade, circumvent or otherwise failing to comply with the principles and

prescriptions contained in the rules, procedures and instructions for the preparation and drafting of financial statements, while ensuring that all accounting entries and records are prepared in such a way as to accurately and fairly reflect the Company's operations;

- return contributions to shareholders or exempt them from the obligation to make them, except in cases of legitimate capital reduction;
- distribute profits, or advances on profits that have not actually been earned or that are allocated by law to legally non-distributable reserves, as well as distribute reserves (even if not established with profits) that may not be distributed by law;
- purchase or subscribe shares of the Company or of companies it may control outside the cases provided for by law, with detriment to the integrity of the share capital;
- carry out reductions in share capital, mergers or demergers, in breach of the legal provisions protecting creditors, causing damage to them;
- proceed in any manner whatsoever to the fictitious formation or increase of the share capital by allocating shares for a value lower than their nominal value when increasing the share capital;
- distribute the company's assets among the shareholders, in the event of any liquidation, before paying the company's creditors or setting aside the sums necessary to satisfy them;
- behave in such a way as to materially impede or otherwise obstruct, through the concealment of documents or the use of other fraudulent means, the performance of control or auditing activities of the management of the company, by the board of statutory auditors or the auditors or the shareholders or, in any case, by other persons in charge of control activities;
- operate in such a way that the completeness, correctness, truthfulness and up-to-dateness of the minutes and documents in which the performance of the Company's activities is reported may be jeopardised, or in such a way as to prepare documentation that is not relevant to the matters under discussion;
- influence the formation of the will of the shareholders' meeting or the passing of resolutions at the meeting through the performance of any simulated or fraudulent act;
- carry out any operation or initiative by failing to inform the Directors and the Board of Statutory Auditors of the existence of a conflict of interest situation, i.e. of any interest of their own in a given Company operation. As far as the Chief Executive Officer is concerned, carry out any operation in conflict of interest without referring it to the collegiate body;
- engage in simulated or otherwise fraudulent transactions, as well as disseminate false or misleading news, rumours or information likely to significantly alter the price of financial instruments.
- omit to make, with due clarity, completeness and timeliness, all the communications, whether periodical or not, required by law and by further sector regulations to the Supervisory Authorities or the transmission of the data and documents required by the rules in force and/or specifically requested by the aforesaid Authorities;
- behave in a way that impedes the exercise of the control and supervisory functions of the above-mentioned persons, including during inspections or when requesting data, information or news;
- evade, circumvent or otherwise fail to comply with the procedure adopted by the Company for the preparation and publication of press releases to be disclosed to the market.

5) Control Principles

The general principles of conduct described in this chapter are aimed at ensuring that the above-mentioned persons, each to the extent to which he/she is entrusted with performing a function within the scope of activities in the risk areas, behave in accordance with precise rules of conduct, in order to prevent and impede the occurrence of corporate offences.

In particular, the recipients of the Model and, in any case, the persons who might commit one of the corporate offences or market abuse offences, each to the extent of his/her competence, are required to know and comply punctually with, in addition to the laws and regulations applicable from time to time the rules and principles contained in the Code of Ethics and in all other documents that the Company has adopted to regulate the activities described above, such as, by way of example but not limited to, the regulations and internal operating instructions to safeguard the correct preparation of the financial statements and, where executed, the interim reports.

The Company guarantees the regular functioning of its own and the corporate bodies, ensuring and favouring any form of internal control deemed appropriate and related to the economic and financial management of the Company, as well as taking care to ensure that the free and correct formation and expression of the will of the shareholders' meeting is always ensured.

For each accounting operation, the Company establishes that documentation of the activity carried out must be kept, so that it can be recorded in the accounts, aimed at allowing the identification of the persons responsible for the various authorisation levels and the reconstruction of the various steps of the operation, in order to be able to clearly assess the responsibility of those who have acted.

All the recipients of the Model must also scrupulously comply with the provisions of the "Procedure for the handling of inside information" adopted by the Company and the rules specified for the proper management of the "Register of persons with access to inside information" adopted by the Company and also published, for their appropriate knowledge and dissemination, on its website.

6) Specific protocols

To supplement the company's Code of Ethics and the principles listed above, TPS has adopted a number of specific protocols in order to raise the level of attention on activities at risk of commission of the offences referred to in Articles 25-ter and 25-sexies of Legislative Decree No. 231/2001.

The protocols identified, whether provided for in the rules or formalised in specific company procedures or policies, are therefore intended to provide greater operational detail to the company functions operating in the processes and activities at risk of these offences being committed.

The Functions involved, the procedures and protocols adopted and the information flows to be forwarded to the Supervisory Board are summarised below.

Organis. Unit/Internal Manager	Documents /Procedures	Protocols	SB flows	Flow Periodicity
Head of Administration, Finance and Control	Po600 - administrative management Procedure for handling inside information Register of persons with access to inside information	Ensuring that the Company's Corporate Functions, sources of accounting information, provide maximum cooperation to the Administration, Finance and Control Manager by respecting the defined closing schedule and following the guidelines for the management of closing activities and the recording/ communication of the required accounting data Restrict access to the database for accounting management to authorised persons only, according to the user profile assigned; ensure that each user has a password linked to a specific access profile in relation to their role Check the outcome of automatic accounting processes and verify the resolution of any anomalies reported by the IT system	Reports on the following subjects: -minutes of the Administrative Body's approval of the draft budgets; -amendments made to the budget at the request of the Administrative Body; -declarations made by Directors and Heads of Department concerning the existence of conflicts of interest; -requests, by anyone, for unjustified variations in the criteria for recognising, recording and representing data in the accounts with respect to those already recorded; -appointments given to external consultants to support the management of the process of drawing up the annual budget, the budget, and extraordinary corporate transactions; -communication concerning extraordinary transactions discussed and/or approved by the Board of Directors and the related feasibility opinion drawn up by the Administration, Finance and Control Officer	Half-yearly

E. Tax offences
(Article 25-quinquiesdecies of Legislative Decree No. 231/2001)

1) Description of the Tax Crimes referred to in Legislative Decree no.

Article 25-quinquiesdecies expressly refers to the commission of the offences specified in Legislative Decree No. 74 of 10 March 2000, which are summarised below:

- fraudulent declaration by use of invoices or other documents for non-existent transactions, provided for in Article 2 par. 1 and par. 2-bis of the aforementioned legislative decree;
- fraudulent declaration by means of other artifices, provided for in Article 3 of the aforementioned legislative decree;
- issue of invoices or other documents for non-existent transactions, as provided for in Article 8 par. 1 and par. 2-bis of the aforementioned legislative decree;
- concealment or destruction of accounting documents, provided for in Article 10 of the aforementioned legislative decree;
- fraudulent evasion of taxes, as provided for in Article 11 of the aforementioned legislative decree.

Paragraph 1-bis of Article 25-quinquiesdecies also makes specific reference to offences committed as part of cross-border fraudulent schemes and for the purpose of evading value added tax for a total amount of at least ten million euro. In particular, the following are indicated:

- false declaration provided for in Article 4 of the aforementioned legislative decree;
- failure to make the declaration provided for in Article 5 of the aforementioned legislative decree;
- undue compensation provided for in Article 10-quater of the aforementioned legislative decree.

2) Identification of sensitive processes and persons involved

TPS considers that there is a risk, to a greater or lesser degree, that the persons indicated in Article 5 par. 1 of the Decree may engage in conduct in violation of the above-mentioned rules, to which, therefore, particular attention was paid in the risk assessment activity and identification of *risk areas / sensitive activities* and related processes.

Having said this, the following *sensitive activities* have been identified (sensitive activities are listed below with the identification number assigned to them in the document entitled Risk Assessment):

- 1.1 Managing relations with the Guardia di Finanza (Tax Police) and Agenzia delle Entrate (Revenue Agency) for tax inspections
- 1.2 Calculating direct and indirect taxes
- 1.3 Tax compliance management: preparing and transmitting telematic data /

tax returns to the tax registry, making the relevant payments and paying taxes (Chamber of Commerce, Guardia di Finanza, Revenue Agency)

- 1.5 Management of receipts and payments (settlement of invoices, etc.)
- 1.6 Cash and treasury management (opening/closing of current accounts; recording of receipts and payments in the general accounts; reconciliation of bank statements and cash transactions; management of the registers of the various company cash desks, etc.)
- 1.7 Management, control and authorisation of advances and reimbursement of expenses to employees and consultants
- 1.8 Management of missions / travels
- 1.9 Valuations and estimates of subjective balance sheet items; recognition, recording and representation of business activities in accounting records, reports, financial statements and other business documents; updating the chart of accounts
- 1.10 Registration of extraordinary transactions (e.g. mergers, acquisitions, etc.)
- 1.11 Disposal of corporate real estate or participations
- 1.13 Preservation of documents over which other corporate bodies could exercise control (e.g. company books, accounting records, etc.)
- 1.18 Checking consistency between purchase invoice and prices, quantity and type of material received in stock
- 1.19 Customer schedule of payments management
- 1.20 Customer and supplier master data management and maintenance
- 1.21 Recording of invoices (receivable and payable) and credit notes
- 1.22 Monitoring of invoices due to be received
- 1.23 Management of the accounting of advance payments to suppliers
- 1.24 Archiving of supporting documentation for invoices issued and received
- 1.25 Management of representation expenses incurred (with PA representatives, with commercial companies or with associations or other non-profit bodies)
- 1.26 Recording the loading and unloading of goods in the warehouse
- 1.27 Electronic invoicing
- 1.28 Back up with computer tools of the accounting archive
- 1.29 Management of fulfilments for obtaining tax benefits (i.e. tax credit, etc.)
- 1.30 Intra-group transactions
- 3.1 Negotiation activities with customers
- 3.2 Determination of contractual conditions and price
- 3.3 Signing of contracts, commercial agreements, framework agreements
- 3.4 Management and maintenance of customer master data: data entry/ updating, commercial and professional customer verification
- 3.5 Management of activities related to the organisation of and/or participation in events for promotion purposes
- 3.6 Sponsorships

- 4.2 Supplier evaluation, qualification and monitoring activities and annual qualification renewal
- 4.3 Contracting and signing purchase contracts with suppliers
- 4.4 Issuing, correcting and updating purchase orders
- 4.5 Awarding of professional and specialist consultancies
- 4.7 Verification of services received with regard to professional appointments and specialist advice to third parties
- 4.8 Contracting out activities to third parties
- 5.9 Delivery of training activities

The recipients of the provisions contained in this section are, therefore, all the corporate functions involved in the processes identified above and, in particular, the Managers and Functions involved in the management of the Company's administrative and accounting fulfilments.

3) Behavioural rules

The principles of conduct and the provisions of the special section apply to all recipients of the Model who are involved in the processes outlined above.

The purpose of the section is to:

- indicate protocols and procedures to be observed for the correct application of the Model;
- provide Area, Process or Function Managers with the list of information flows to be transmitted to the Supervisory Body in charge of carrying out verification and control activities.

For this purpose, it is required to:

- observe the rules and principles of the company's Code of Ethics;
- maintain a correct and transparent conduct, ensuring full compliance with the law, regulations and corporate procedures in the performance of all activities aimed at drawing up the financial statements, periodic accounting situations and other corporate communications. All this in order to provide shareholders, creditors and third parties with a correct and clear representation of the Company's equity, economic and financial situation;
- make prompt, correct and complete all communications required by law and regulations to the public supervisory authorities, not obstructing in any way the exercise of their functions;
- establish and maintain any relationship with the Control Bodies and corporate third parties on the basis of criteria of utmost fairness and transparency.

It is expressly forbidden to:

- engage in conduct that may constitute, directly or indirectly, one of the offences under Article 25-quinquiesdecies of Legislative Decree 231/2001;
- engage in conduct in breach of the rules of conduct and company procedures;
- communicate erroneous data and information concerning the economic, asset and financial situation of the Company, in order to obtain an undue advantage in the calculation of tax and fiscal liabilities;
- fail to comply with the principles and prescriptions contained in the

instructions for the preparation of financial statements, the general accounting plan and the industrial accounting manual;
- behave in such a way as to materially impede, or in any case hinder, through the concealment of documents or the use of other fraudulent means, the performance of control or auditing activities of the company management by the Board of Statutory Auditors, the Auditing Firm or the Shareholders;
- fraudulently issue invoices for non-existent transactions or concealing and destroying accounting documents;
- fail to make, with due clarity, completeness and timeliness, the necessary communications to the authorities in question;
- engage in any conduct that is an obstacle to the exercise of functions by the public supervisory authorities, including during inspections: for example, express opposition, pretextual refusals, obstructive behaviour or non-cooperation, such as delays in communications or in the provision of documents.

4) Specific Protocols

To supplement the corporate Code of Ethics and the principles listed above, TPS has adopted a number of specific protocols in order to raise the level of attention on the activities at risk of commission of the offences referred to in Article 25-quinquiesdecies of Legislative Decree no. 231/2001.

The protocols identified, whether provided for in the rules or formalised in specific company procedures or policies, are therefore intended to provide greater operational detail to the company functions operating in the processes and activities at risk of these offences being committed.

The corporate processes concerned, the Functions involved, the procedures and protocols adopted and the information flows to be forwarded to the Supervisory Board are summarised below.

• Procurement Process for Goods and Services

Organis. Unit/Internal Manager	Documents /procedures	Protocols	SB flows	Flow Periodicity
Procurement Management Purchasing Office	Po300 - supply man-agement Po301 - general conditions of purchase	Inclusion in work orders and supply contracts of a clause on compliance with the Code of Ethics and the Model. Dissemination of the Model and Code of Ethics to employees and periodic training	List of suppliers, professional appointments and consultancies.	Yearly

• **Process for managing active invoicing of services provided**

Organis. Unit/Internal Manager	Documents /Procedures	Protocols	SB flows	Flow Periodicity
Commercial Management Administration, Finance and Control Department Administration Office	Po200 - business process management Po600 - administrative management	Inclusion in commercial offers of a clause on compliance with the Code of Ethics and the Model. Dissemination of the Model and Code of Ethics to employees and periodic training	Reporting any complaints about invoicing procedures (transparency).	Event-driven

• **Accounting and Administrative Management Process**

Organis. Unit/Internal Manager	Documents /Procedures	Protocols	SB flows	Flow Periodicity
Administration, Finance and Control Department Administration Office	Po600 - administrative management	Specific training of administrative staff on corporate offences Dissemination of the Model and Code of Ethics to employees and periodic training Annual coordination with audit activities conducted by the Audit Board.	Copy of the approved financial statements. VAT and UNICO tax returns.	Yearly

F. Offences relating to health and safety es of Legislative Decree no. 231/2001)

1) Identification of risk areas, sensitive processes and persons involved

Article 25-septies of Legislative Decree no. 231/2001 introduced the provision of administrative sanctions against the Entities and legal persons referred to in the Decree for cases of homicide or serious or very serious culpable lesions committed in violation of occupational health and safety regulations.

Therefore, in addition to the other offences contained in the Decree, for which the existence of wilful misconduct on the part of the agent is required, the Article in question introduces a number of offences for which the agent is also liable by way of negligence, specifically specific negligence (referring in particular to the violation of the rules of conduct imposed by the observance of rules of experience, later codified in laws, regulations or disciplines such as the "Rules on the protection of health and safety at work", contained in Legislative Decree no. no. 81 of 30 April 2008, hereinafter also referred to as "Consolidated law on safety at work", which reorganises and coordinates in a single regulatory text the existing rules on workers' health and safety.

The active parties who can abstractly commit the offences referred to in the decree are:

- Employer, who is the main actor in the field of prevention and protection;
- Supervisor;
- Prevention and Protection Service Manager, on a residual and concurrent basis;
- Person who has de facto assumed, albeit in clear disregard of the Model and the internal regulations of the Company, a position of "guarantee" within the meaning of Article 299 of Legislative Decree no. 81/2008.

As regards the identification of risk areas, first of all we consider those in which an event (death or injury) could occur that the above-mentioned regulations aim to prevent.

In this respect, although, in the abstract, any accident could occur in any occupation to which a worker is assigned, the activities carried out by TPS are such that the risk of a serious or very serious event is low, bordering on insignificant.

In fact, the company conducts activities that qualify as "office" activities, so that the employees and managers assigned to them are hardly exposed to the risk of harm to their health.

On the other hand, a further area of risk is that of the concrete fulfilment of the legal obligations contained in the regulations on health and safety at work, because the Company, as a result of the omission or ineffective implementation of these obligations, could incur the culpable liability provided for in Legislative Decree No. 231/2001.

That said, with reference to the areas of risk, the following sensitive processes can be identified, by way of example and not exhaustively:

- risk assessment;
- identification and appointment of the RSPP;
- identification and appointment of the occupational health physician;
- identification and appointment of supervisors;
- identification and definition of protective measures;
- checks on workers' training, outsourcing of work, purchases of equipment, machinery and plant, and compliance with company directives;
- management of working environments and emergencies;
- assignment and maintenance of PPE.

TPS, in order to prevent the occurrence of the conduct described above, hypothetically productive of damage and capable of giving rise to the liability of the legal person, has set up a Risk Management System articulated first of all in the assessment of risks, in accordance with the provisions of the regulations on the subject, and then in the provision to observe the content of the general rules and special rules dictated with reference to sensitive processes.

That being said, the Company has chosen the figure of the Employer, pursuant to the provisions of the Consolidation Act, identifying the person of the Managing Director for this purpose. In addition, it adopted the Risk Assessment Document (also RAD), aimed at identifying risks and preparing the collective and individual prevention and protection measures deemed appropriate in relation to each sector or work area and for each category of workers.

The conduct that could constitute the offences described in this section could in abstract constitute the most problematic category among those examined in the Model, even though, as already stated, for the specific activity carried out by TPS, they constitute a "low" risk.

2) Special rules of conduct to be observed in risk areas

The guiding principle of the entire company policy on accident prevention and worker protection is that of maximum accountability of all those who, at different levels, with various tasks and each according to their attributions and competences, work within TPS, without forgetting even third parties, who may be contracted to carry out works.

Consequently, as safeguards, first and foremost, TPS establishes the express prohibition for all recipients of the Model to engage in or even merely tolerate others engaging in conduct in breach of the provisions of Legislative Decree No. 81/2008, i.e. such as to integrate the elements of the types of offences that this legislation aims to prevent.

It is also forbidden to engage in conduct that might compromise the safety precautions adopted by the Company, contributing to the potential commission of the offences of culpable homicide and culpable personal injury.

It is then absolutely forbidden to perform actions that do not comply with company procedures or, in any case, conduct that is not in line with the principles expressed in this Model.

In more analytical terms, but still by way of example and not exhaustively, in the context of TPS the main figures of reference under Legislative Decree no. 81/2008 carry out the following activities:

EMPLOYER

a) provides for the assessment of risks to the safety and health of workers, with all the consequences in terms of the choice of machinery, equipment and organisation of the activity, so that the working environment complies with the principles and criteria in accordance with the law;
b) the above-mentioned assessment is expressed in the risk assessment document (RAD), drafted in such a way as to identify the prevention and protection measures to be adopted and any individual protection devices to be provided to workers, planning any appropriate measures to ensure the improvement of safety levels over time;
c) chooses and appoints the Prevention and Protection Service Manager (RSPP) and the occupational health physician, so that all the requirements of professionalism and experience required by law are met.

SUPERVISOR

specifically instructed by the Employer:

a) supervises the operational activity and the behaviour of the workers during the activity;
b) ensures that everyone works in accordance with the applicable regulations and the requirements imposed by the RAD;
c) provides workers with the personal protective equipment specified in the RAD for each specific activity;
d) monitors machinery, plant, other work equipment, safety devices and workplaces, promptly reporting any need for intervention or adaptation.

Prevention and Protection Service Manager

a) takes care of updating the risk assessment and prevention measures in relation to organisational and production changes that are relevant to occupational health and safety, or in relation to the degree of development of prevention and protection technology;
b) ensures that workers are assigned tasks and duties commensurate with their abilities and condition;
c) ensures that workers are provided with the necessary personal protective equipment and that measures are taken so that only those workers who have been adequately trained can have access to production areas that expose them to specific risks;
d) supervises to ensure that individual workers, who must be trained following special courses and adequately informed, act in strict compliance with the applicable rules and company regulations on occupational safety and hygiene and make use of the collective means of protection and individual protective equipment made available to them.

OCCUPATIONAL HEALTH PHYSICIAN

a) schedules health surveillance in consultation with the employer, keeping up-to-date health records of workers;
b) visits the workplace at least once a year or at different intervals depending on the risk assessment;
c) takes part in the periodic meeting referred to in Article 35 of Legislative Decree No. 81/2008 and communicates the anonymous results of the health surveillance carried out by him/her, illustrating the significance of the results for the implementation of the measures for the protection of the health and integrity of Workers.

WORKERS' SAFETY OFFICER (RLS)

a) can promote the development, identification and implementation of preventive measures to protect the health and psychophysical integrity of workers;
b) participates in the "periodic risk prevention and protection meeting" referred to in Article 35 of Legislative Decree No. 81/2008;
c) is consulted at the time of risk assessment and the planning and implementation of measures for the implementation of preventive measures to protect the health and integrity of workers.

WORKERS

a) must observe the provisions and instructions given to them by the Employer and the Supervisors aimed at their collective and individual protection;
b) must use machinery, plant, other work equipment and safety devices in the intended and appropriate manner;
c) must always use the protective equipment made available to them in the intended and appropriate manner;
d) must immediately report to the Employer or the Supervisors about any problem occurring or registered on the means, plant, equipment described above and in the workplace, as well as any other dangerous condition they become aware of, also informing the Workers' Safety Representative;
e) may never remove or modify security or signalling or control devices without authorisation;
f) must not carry out on their own initiative any activities or manoeuvres that are outside their competence or that may jeopardise their safety or the safety of others;
g) must participate in the training and instruction programmes organised by the Employer, and also undergo the health checks provided for them;
h) must contribute, together with the Employer and the Supervisors, to the fulfilment of all obligations imposed by the competent authority or otherwise necessary to protect the safety and health of Workers at work.

TPS makes use of a set of procedures, of operating instructions consisting of technical standards, of good working practices all complying with the standards in force, of information and training activities aimed at making workers learn the correct use of equipment, machines, plants, substances and protective devices, including individual ones.

Verbal information and instructions are transferred by the Supervisors in a non-formalised manner, directly at the workplace in the course of work, taking care that they are well understood by those receiving them.

The health and safety risks associated with the activity developed by the Company in general and the specific risks associated with the individual task assigned and, therefore, the relevant prevention and protection measures adopted by the Company are suitably disclosed by the latter, as are the contents of the relevant regulations, obligations, responsibilities and duties, as well as the contents of the specific safety procedures.

This training course continues with specific training carried out by the worker alongside more experienced colleagues, under the supervision of the Supervisor, while in the case of a change of job, the worker is guaranteed a similar training course.

Refresher training activities are subject to specific periodic planning depending on the development or the regulatory framework of reference and or the equipment, materials and technologies used in the production process.

Within the framework of the aforementioned planning, the Employer schedules the specific refresher training for those who have management tasks in this field, such as the Prevention and Protection Service Manager (when internal to the organisation), the Workers' Safety Representatives, the Supervisors and the Workers.

In the context of the periodic safety meetings, the Employer and the Prevention and Protection Service Manager ensure that the collective anonymous results of the health surveillance carried out are communicated and discussed, and that indications are given as to their significance, so that measures for the protection of the health and psycho-physical integrity of workers can be implemented.

The recipients of this section must exercise continuous and punctual control aimed at highlighting risks that could entail the commission of the offences specified in Article 25-septies and, in general, any situation that could entail a danger to the hygiene and health of workers and of all persons in any case present in the areas of the Company.

3) Specific Protocols

To supplement the company's Code of Ethics and the principles listed above, TPS has adopted a number of specific protocols in order to raise the level of attention on activities at risk of commission of the offences referred to in Article 25-septies of Legislative Decree No. 231/2001.

The protocols identified, whether provided for in the rules or formalised in specific company procedures or policies, are therefore intended to provide greater operational detail to the company functions operating in the processes and activities at risk of these offences being committed.

The corporate processes concerned, the Functions involved, the procedures and protocols adopted and the information flows to be forwarded to the Supervisory Board are summarised below.

Organis. Unit/Internal Manager	Documents /Procedures	Protocols	SB flows	Flow Periodicity
Employer / Prevention and Protection Service Manager	Risk Assessment Document Integrated Management System Manual	Special rules of conduct to be observed in the risk areas identified in this Special Section	Reports on the following subjects: -updates to the RAD (risk assessment document) and DUVRI (single document on the assessment of risk from interference); -number and subject of training courses carried out, -updates and implementations of safe work procedures and instructions; -fines imposed for non-compliance with accident prevention requirements; -inspections that may have taken place and formalised observations by inspectors in the field of health and safety at work; -annual plan of activities and audits to be carried out in the current year (at the time of sending the report) and the timeframe for their implementation -activity carried out and the controls performed according to the annual activity plan of the previous year (to that of the report submission); -brief report on the state of adequacy and effective implementation of the measures provided for in the RAD;	Yearly

G. Offences of inducement not to make statements or to make false statements to the judicial authorities

The conduct referred to in Article 25-decies of Legislative Decree no. 231/2001 and specified in Article 377-bis of the Criminal Code consists of inducing someone not to make statements or to make false statements to the Judicial Authorities.

The risk areas that TPS has identified are those pertaining to the management of the Company's pending litigation in the various fields of civil, criminal, administrative and any other law.

TPS strictly forbids any recipient of the Model to act contrary to the provisions of Article 377-bis of the Criminal Code, stating that it is absolutely forbidden to interfere, or even to attempt to do so, with the content of the statements that any person may be called upon to make before the Judicial Authorities, in order to induce anyone not to make statements or to make false statements.

Sensitive processes can be identified in any relationship that any subject among the recipients of the Model may have with the Judicial Authority, subjects delegated by the latter in any civil, criminal or administrative proceedings.

Having said this, the following *sensitive activities* have been identified (sensitive activities are listed below with the identification number assigned to them in the document entitled Risk Assessment):

- 1.14 Management of Relations with Shareholders and the Supervisory Board
- 1.15 Debt collection activities
- 2.3 Litigation management, coordination of legal advisers, filing of documents

The main safeguard for the prevention of the aforementioned conduct is constituted, in addition to the rules of the Code of Ethics, by the internal sanctioning system adopted by the Company, which will not hesitate to penalise, in accordance with the procedures and to the extent provided for, the person who engages in the prohibited conduct.

H. Offence of employment of irregular workers from third countries

1) Identification of risk areas, sensitive processes and persons involved

The case in question is referred to in Article 25 duodecies of the well-known Legislative Decree. Lgs. which is referred to in Article 22 paragraph 12-bis of Legislative Decree no. 286/1998.

The latter prohibits the employment of persons who have irregularly entered the State from so-called third countries and therefore without a regular residence permit.

To be more precise, the aforementioned Art. 22 paragraph 12-bis expressly mentions the hypotheses of the "employer who employs foreign workers without a residence permit provided for in this article, or whose permit has expired and whose renewal, revocation or cancellation has not been requested, within the terms of the law" in cases in which "a) the workers employed are more than three; b) the workers employed are minors of non-working age; c) the workers employed are subject to other particularly exploitative working conditions referred to in the third paragraph of Article 603-bis of the Criminal Code"

It is easy to see how the area of risk can be identified in relations with subordinate workers and the sensitive processes can be summarised as follows:

- contacts and interviews when planning to hire non-EU workers;
- ascertaining the foreign worker's place of origin through his/her documents;
- ascertaining the existence, where necessary, of a valid residence permit and checking its duration,
- preparation and signing of the employment contract.

Having said this, the following *sensitive activities* have been identified (sensitive activities are listed below with the identification number assigned to them in the document entitled Risk Assessment):

- 2.4 Process management of:

  1) personnel selection
  2) recruitment of employees

- 4.8 Contracting out activities to third parties

Those potentially involved are those involved in the Human Resources Management procedure (PO400). In particular, the Human Resources Director is mentioned.

2) Rules of conduct to be observed in sensitive processes and their safeguards

TPS, from the very beginning of the first job interview, must carefully ascertain the origin of the foreign worker and, in the case of a non-EU subject, the person in charge must ascertain the worker's lawful presence in the State by requiring a valid residence permit. The permit must be valid for the entire assumed duration of the relationship to be established or, otherwise, the employment contract must explicitly provide that the reiteration of the validity of the residence permit before its expiry constitutes an essential element for the continuation of the relationship between TPS and the worker.

In the event of a renewal or extension of the relationship, the worker must first present the renewal of the residence permit.

The safeguards in place include, in addition to the general ones adopted by the Company with the Code of Ethics, the Human Resources Management procedure (PO400) and this chapter.

3) Specific Protocols

To supplement the company's Code of Ethics and the principles listed above, TPS has adopted a number of specific protocols in order to raise the level of attention on activities at risk of commission of the offences referred to in Article 25 duodecies of Legislative Decree No. 231/2001.

The protocols identified, whether provided for in the rules or formalised in specific company procedures or policies, are therefore intended to provide greater operational detail to the company functions operating in the processes and activities at risk of these offences being committed.

The corporate processes concerned, the Functions involved, the procedures and protocols adopted and the information flows to be forwarded to the Supervisory Board are summarised below.

Organis. Unit/Internal Manager	Documents /Procedures	Protocols	SB flows	Flow Periodicity
Human Resources Manager	Integrated Management System Manual and, in particular, the PO400 and all other procedures and references referred to therein	Rules of conduct to be observed in sensitive processes and related controls identified in this Special Section	Reports on the following subjects: - list of possible recruitments of workers from third countries (see Article 22 par. 12-bis of Legislative Decree no. 286 of 25 July 1998)	Yearly

Periodic checks and monitoring activities entrusted to the supervisory body

The Supervisory Board (SB) performs its function in compliance with the provisions specified in Legislative Decree No. 231/2001, in the 231 Model adopted by the Company and in the "Articles of Association of the Supervisory Board" (also regulated in the General Section of the Model).

In particular, the Supervisory Board has the task of carrying out key second-level controls:

- verify the observance, implementation and adequacy of the Model (General Section and Special Section) with a view to preventing the commission of the offences identified in this protocol;
- supervise the effective application of the General Section and the Special Section of the Model and detect any behavioural deviations of the recipients if found by the analysis of information flows and reports received;
- receive and process reports of violations of the 231 Model (or of other offences relevant to the Company as governed by Legislative Decree no. 24/2023) in compliance with the Whistleblowing Procedure adopted by the Company;
- periodically check, with the support of the functions deemed necessary, the system of delegated and proxy powers and the authorisation system in force;
- periodically verify compliance with the principle of separation of functions within the individual operational areas and, in particular, with regard to the sensitive activities detected;
- verifying compliance with existing operating procedures on sensitive areas;
- take care of updating the Model.

The Supervisory Board then communicates the results of its supervisory and control activities to the Administrative Body, in accordance with the terms specified in the Articles of Association of the Supervisory Board.

Information flows to the supervisory body

In order to enable the Supervisory Board to supervise the effective operation of and compliance with the Model and to keep it up-to-date, a constant exchange of information between the recipients of the Model and the Supervisory Board must be defined and implemented.

In particular, as already referred to in greater detail in the specific paragraph 5.5 of the General Section, the Organisation, Management and Control Model adopted by the Company identifies the following **three types of information flows** addressed to the Supervisory Board:

A) PERIODIC INFORMATION FLOWS,

to be sent using the e-mail address: *odv@tps-group.it*

The obligation to provide periodic information flows is addressed primarily to the structures deemed to be at risk in terms of the potential risk of commission of the offences provided for in the Legislative Decree no. 231/2001.

In order to create a complete and constant management system of information flows to the Supervisory Body, for each area at risk of offence and for each instrumental area, the Company has identified a **person responsible for sending the flows**, who assumes, by signing a specific binding commitment, the obligation to transmit standardised reports to the Supervisory Body, the subject of which is specifically determined in the following paragraph of this Special Section entitled "Details of periodic information flows".

The **person responsible for sending the flows** ensures the collection of information, its initial examination, its systematisation into explicit information reports and finally its transmission to the Supervisory Board.

B) OCCASIONAL INFORMATION FLOWS ("EVENT-DRIVEN"),

also to be sent using the e-mail address: *odv@tps-group.it*

Also in this case, as for the previous type of flow, in order to create a complete and constant management system of information flows towards the Supervisory Board, for each event to be reported the Company has identified, where possible, a **person responsible for sending**the flows, addressing - in the residual hypotheses for which a direct person responsible for sending the flows cannot be immediately identified - this reporting obligation to **all the recipients of** the Model itself.

C) REPORTS OF VIOLATIONS OF MODEL 231 (OR OF OTHER OFFENCES RELEVANT TO THE COMPANY AS GOVERNED BY LEGISLATIVE DECREE 24/2023),

to be sent using the communication channels indicated in the Whistleblowing Procedure, which can be found in full in the following link:

https://www.tps-group.it/investor-relations section "Business Ethics"

The obligations to inform the Supervisory Board, in its capacity as the manager of the reports received through the Whistleblowing Procedure, also concern any further information concerning violations of the 231 Model or the commission, even if alleged, of other offences relevant to the Company as defined in the aforementioned reporting procedure (so-called whistleblowing reports)

Detail of periodic information flows

A) OFFENCES IN RELATIONS WITH THE STATE, PUBLIC BODIES AND THE EUROPEAN UNION

(Articles 24 and 25 of Legislative Decree No. 231/2001)

Description of the information flow	Periodicity	Head of Department
Reports on the following subjects: - list of visits, inspections and audits initiated or concluded during the reporting period, with an indication of the respective findings; - copies of the minutes of the inspections that were concluded with non-compliances and findings and sanctions imposed, if any.	Half-yearly	Head of the Department involved in the inspection
Reports on the following subjects: - list of ongoing proceedings; - list of out-of-court settlements (criminal, civil and administrative litigation) signed by the Company or in the process of being settled; - list of assignments given to lawyers and the progress of judicial and/or extrajudicial activities.	Half-yearly	Head of Staff Management

B) COMPUTER CRIMES AND ILLICIT DATA PROCESSING; CRIMES RELATING TO INFRINGEMENT OF COPYRIGHT

(Article 24-bis and Article 25-nonies of Legislative Decree No. 231/2001)

Description of the information flow	Periodicity	Head of Department
Reports on the following subjects: - up-to-date inventory of software in use by the Company and its licences; - copies of contracts governing relations with outsourcing service providers / IT consultants.	Yearly	IT infrastructure and software manager

C) CRIMES OF COUNTERFEITING MONEY, RECEIVING STOLEN GOODS, MONEY LAUNDERING, USE OF MONEY, GOODS OR BENEFITS OF UNLAWFUL ORIGIN

(Articles 25-bis and 25-octies of Legislative Decree no. 231/2001)

Description of the information flow	Periodicity	Head of Department
Reports on the following subjects: - list of anomalous transactions for anti-money laundering purposes, suspended for having activated the authorisation procedure required by the protocol indicated in paragraph c) above, referring to the "offences of counterfeiting currency, offences of receiving stolen goods, money laundering, use of money, goods or utilities of unlawful origin" of this special section	Yearly	Head of Administration, Finance and Control

D) CORPORATE OFFENCES; MARKET ABUSE

(Article 25-ter and Article 25-sexies of Legislative Decree No. 231/2001)

Description of the information flow	Periodicity	Head of Department
Reports on the following subjects: - minutes of the Administrative Body's approval of the draft budgets; - amendments made to the budget at the request of the Administrative Body; - declarations made by Directors and Heads of Department concerning the existence of conflicts of interest; - requests, by anyone, for unjustified variations in the criteria for recognising, recording and representing data in the accounts with respect to those already recorded; - appointments given to external consultants to support the management of the process of drawing up the annual budget, the budget, and extraordinary corporate transactions; - communication concerning extraordinary transactions discussed and/or approved by the Board of Directors and the related feasibility opinion drawn up by the Administration, Finance and Control Officer	Half-yearly	Head of Administration, Finance and Control

E) TAX OFFENCES

(Art. 25-quinquiesdecies of Legislative Decree no. 231/2001)

Description of the information flow	Periodicity	Head of Department
List of suppliers, professional appointments and consultancies.	Yearly	Procurement Management
Copy of the approved financial statements. VAT and UNICO tax returns.	Yearly	Head of Administration, Finance and Control

F) OFFENCES RELATING TO HEALTH AND SAFETY AT WORK

(Article 25-septies of Legislative Decree no. 231/2001)

Description of the information flow	Periodicity	Head of Department
Reports on the following subjects: - updates to the RAD (risk assessment document) and DUVRI (single document on the assessment of risk from interference); - the number and subject of training courses carried out; - updates and implementations of safe work procedures and instructions; - fines imposed for non-compliance with accident prevention requirements; - inspections that may have taken place and formalised observations by inspectors in the field of health and safety at work; - annual plan of activities and audits to be carried out in the current year (at the time of sending the report) and the timeframe for their implementation - activity carried out and the controls performed according to the annual activity plan of the previous year (to that of the report submission); - brief report on the state of adequacy and effective implementation of the measures provided for in the RAD	Yearly	Employer / Prevention and Protection Service Manager

G) OFFENCES OF INDUCEMENT NOT TO MAKE STATEMENTS OR TO MAKE FALSE STATEMENTS TO JUDICIAL AUTHORITIES

For the type of offence risk under this heading, only occasional information flows are envisaged (so-called "event-driven").

H) OFFENCE OF EMPLOYMENT OF IRREGULAR WORKERS FROM THIRD COUNTRIES

Description of the information flow	Periodicity	Head of Department
Reports on the following subjects: - list of possible recruitments of workers from third countries (see Article 22 par. 12-bis of Legislative Decree no. 286 of 25 July 1998)	Yearly	Human Resources Manager

Detail of occasional information flows ("event-driven")

Description of the information flow	Periodicity	Head of Department
Participation in public tenders or competitions at national and international level of the and any findings;	At the event feedback	General Manager
Transactions relating to matters concerning "predicate" offences in the case of relations with countries on the so-called "black list"	At the event feedback	General Manager
The transactions, if any, considered anomalous for anti-money laundering purposes, to be suspended in order to activate the authorisation procedure required by the protocol indicated in paragraph c) above, referring to the "offences of counterfeiting currency, receiving stolen goods, money laundering, and use of money, goods or utilities of unlawful origin" of this special section	At the event feedback	Head of Administration, Finance and Control
The commencement of any control or inspection activity affecting the Company, for which minutes must be drawn up of the entire inspection process	At the event feedback	Head of Staff Management
Changes made to existing delegations and/or the issuance of new ones, with details of their specific contents	At the event feedback	Head of Staff Management
Reports or requests for legal assistance forwarded to the Company by senior managers or persons subject to the direction of others in the event of legal proceedings being brought against them for one of the offences provided for in the Decree	At the event feedback	Head of Staff Management
Requests for legal assistance, sent by employees or collaborators, concerning the commencement of investigations or legal proceedings against them concerning offences under the Decree, unless expressly prohibited from disclosure by the judicial authorities	At the event feedback	Head of Staff Management
Application for, disbursement and use of public funding	At the event feedback	Head of Administration, Finance and Control

Description of the information flow	Periodicity	Head of Department
Reporting any complaints about invoicing procedures (transparency)	At the event feedback	Head of Administration, Finance and Control
Changes to the company structure, its organisational chart (including administrative and commercial areas)	At the event feedback	Human Resources Manager
Any reports prepared by the various managers as part of their control activities, from which facts, acts or omissions with critical profiles may emerge with respect to compliance with the provisions of the Decree or the provisions of the Model	At the event feedback	All recipients of the Model
The emergence of new risks in the areas directed by the various managers	At the event feedback	All recipients of the Model
Any anomalies, atypicalities detected or findings by the corporate functions of the control activities put in place to implement the Model	At the event feedback	All recipients of the Model
Measures and/or information from judicial police bodies, or from any other public authority, from which it can be inferred that investigations for the offences referred to in the Decree have been carried out, even against unknown persons	At the event feedback	All recipients of the Model
Internal reports from which responsibility for the alleged offences emerges	At the event feedback	All recipients of the Model
Communications, measures, deeds, sentences, decisions and anything else that may be assimilated therewith from judicial bodies of any kind and degree, even against unknown persons, for the "predicate" offences contemplated by the Decree that may potentially involve the Company	At the event feedback	All recipients of the Model
The existence of conduct that is even potentially contrary to the adopted Model	At the event feedback	All recipients of the Model

TPS S.p.A.
Sede legale: Via Lazzaretto, 12/c – Gallarate (VA)

www.tps-group.it